Elementos de Matemática Discreta

Antonio De Jesús Bonilla Bonilla[1]

Universidad Autónoma de Santo Domingo
Facultad de Ciencias
Escuela de Matemática
[1]Profesor titular escuelas Matemática e Informática

Enero del 2016

Contenido

Contenido

Contenido

Contenido

Contenido



La **matemática discreta** es la rama de la matemática que tiene por objeto el estudio de conjuntos discretos (finitos o infinitos numerables). Es lo contrario a la **matemática continua**, que se fundamenta en el conjunto de los reales y que estudia conceptos como límites, continuidad, etc.

La matemática discreta estudia objetos como gráficas, lógica, etc., cuyos elementos pueden ser contados o tratados uno a uno, separadamente. Es decir, la matemática discreta tiene como base fundamental al conjunto de los enteros.

El lenguaje que usamos a diario suele ser poco claro y de precisión dudosa y nuestra forma de pensar a veces se hace confusa. De aquí

que la lógica desde sus inicios se ha convertido en una herramienta que tiende a disciplinarnos en el uso del lenguaje y el pensamiento. No es posible concebir el estudio de alguna actividad humana sin entender la importancia de la lógica en dicho proceso.
La lógica junto la teoría de conjuntos tocan transversalmente todas las ramas del saber. La teoría de conjuntos juega un papel importante en la formación básica de los futuros profesionales de las áreas de ciencias y tecnologías.

¿Por qué estudiar Lógica?

EL lenguaje que usamos a diario nos conduce muchas veces a ambigüedades que permiten hacer interpretaciones distintas y desde

el punto de vista de la lógica, esto es inaceptable. Por esta razón, la ciencia utiliza un lenguaje diferente que evite las ambigüedades y que sea universal. De aquí que la lógica viene a llenar este vacío, porque aunque utiliza un lenguaje simbólico, es más preciso y exacto que el lenguaje común.

Contenido

La palabra **lógica** proviene de la palabra griega LOGOS, que significa pensamientos correctos. El adjetivo “formal” se refiere a que la lógica trabaja en base a la razón pura, independientemente de la experiencia que se tenga, es decir, prescindiendo del contenido del pensamiento.

El estudio de la informática y/o matemática para cualquier estudiante es mucho más interesante y provechoso, si previamente se le introduce en el mundo de la lógica formal.
El manejo del lenguaje lógico y el uso de procedimientos eficientes de razonamiento son elementos que contribuyen significativamente al desarrollo de algoritmos computacionales de calidad.

La **lógica** tiene por objeto estudiar la validez de los razonamientos.

Contenido

Empecemos ofreciendo algunas definiciones que serán útiles a nuestros propósitos.

Un **razonamiento** es el proceso mental que nos permite obtener conclusiones partiendo de declaraciones dadas previamente. La lógica trabaja con dos tipos de razonamientos: el **razonamiento material** que se basa en el estudio de la validez de los contenidos de las expresiones tratadas; y el **razonamiento formal** que estudia la validez de las expresiones construidas basada en la razón pura y mediante reglas formales establecidas.

En el lenguaje ordinario utilizamos normalmente cuatro tipos de oraciones: declarativas, interrogativas, exclamativas e imperativas. De estas, nos interesa trabajar básicamnete con las declarativas.
Una **proposición** es una oración declarativa, de la cual se pueda afirmar que su contenido es verdadero o falso, pero no ambas cosas a la vez. Es decir, las proposiciones tienen un único valor de verdad. Se llama **valor de verdad** de una proposición a la verdad o falsedad de la misma.

Por ejemplo, las oraciones siguientes son proposiciones:

1. Pedro es inteligente y estudioso
2. Bogotá es la capital de Colombia
3. Hoy está lloviendo

Las proposicones pueden ser: **simples (atómicas)** o **compuestas (moleculares)**. Se llaman **proposiciones simples** aquellas que constan de sólo un sujeto y sólo un predicado y debe ser afirmativa. Se llaman **proposiciones compuestas** aquellas que están formadas por dos o más proposiciones simples enlazadas entre si por medio de ciertos elementos llamados **operadores o conectivas lógicas** (“no”, “y”, “o”, “si . . . , entonces . . . ”, “si y sólo si”).
Ejemplos de proposiciones simples.

1. Lima es la capital de Perú.
2. 9 es un número primo.
3. Hoy está lloviendo.
4. Un triángulo tiene tres lados.

La proposición “Juan no es artista” no es una proposición simple por ser un juicio de otro juicio.

Ejemplos de proposiciones compuestas.

1. 2 es un número primo y par.
2. Felipe es inteligente y afortunado.
3. Juan es profesor o artista.
4. Andrés y Antonio son deportistas.
5. Si un triángulo es equilátero, entonces es isósceles.
6. O Luis es militar o es médico.

variable proposicional: es un símbolo que contiene una proposición y generalmente se representa por letras minúsculas como $p, \; q, \; r, \; s, \; t,$ etc.

Por ejemplo, consideremos las proposiciones:

p: "2 es un número primo"

q: "2 es un número par"

La proposición: "2 es un número primo y par" puede ser escrita como: "p y q".
De la misma manera, la proposición: "2 no es un número primo ni par" puede escribirse como: "no p y no q".

Operador monádico: es aquel que afecta solamente a una proposición atómica. La negación es el único operador monádico y lo simbolizaremos por $\neg$.

Operador diádico: es aquel que afecta a dos proposiciones atómicas o moleculares.

Tablas de verdad: Son arreglos de filas y columnas donde se representan todas las combinaciones posibles de los valores de verdad de las proposiciones simples que forman las proposiciones compuestas y el valor de verdad de cada combinación.

Negación

La negación de una proposición se obtiene anteponiendo a la proposición las expresiones: “Es falso que”, “No es verdad que” o insertando la partícula “no” en la proposición cuando sea posible.

Si una proposición es verdadera, su negación es falsa y viceversa.

La tabla de verdad de la **negación** es

p	$\neg p$
V	F
F	V

Conjunción

La conjunción es una proposición compuesta formada por dos proposiciones simples, enlazadas por el operador “y” ($\wedge$) y que es verdadera sólo cuando las dos proposiciones son verdaderas; en cualquier otro caso es falsa.
La tabla de verdad de la conjunción es:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Disyunción inclusiva

La disyunción inclusiva es una proposición compuesta formada por dos proposiciones simples, enlazadas por el operador “o” ($\vee$) y que es falsa sólo cuando ambas proposiciones son falsas; en cualquier otro caso es verdadera. A esta disyunción también se le llama **disyunción débil**.

La tabla de verdad de la disyunción inclusiva es:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Disyunción exclusiva

La disyunción exclusiva es una proposición compuesta formada por dos proposiciones simples, enlazadas por el operador "o...o" ($\veebar$) y que es falsa sólo cuando ambas proposiciones tienen el mismo valor de verdad; en cualquier otro caso es verdadera. A esta disyunción se le llama **disyunción fuerte**.
La tabla de verdad de la disyunción exclusiva es:

p	q	$p \veebar q$
V	V	F
V	F	V
F	V	V
F	F	F

Condicional

La implicación o condicional es una proposición compuesta formada por dos proposiciones simples, enlazadas por el operador "Si ... entonces ..." ($\rightarrow$). En esta conectiva hay que distinguir dos partes:

"Si ...": recibe el nombre de **antecedente o hipótesis**

"entonces ...": recibe el nombre de **consecuente o conclusión**

En muchas ocasiones el "Si" y el "entonces" están sobreentendidos o sustituidos por otros términos equivalentes. La condicional es falsa sólo cuando el antecedente es verdadero y el consecuente es falso; en cualquier otro caso es verdadera.

La tabla de verdad de la condicional es:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

En $p \to q$ decimos que p es condición suficiente para q y que q es condición necesaria para p.

Bicondicional o doble condicional

La bicondicional o doble condicional es una proposición compuesta formada por dos proposiciones simples, enlazadas por el operador "...

si y sólo si ...” ($\leftrightarrow$) y que es verdadera sólo cuando ambas proposiciones tienen el mismo valor de verdad; en caso contrario es falsa.

La tabla de verdad de la bicondicional es:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

El número de filas en una tabla de verdad viene dado por 2^n, donde n es la cantidad de proposiciones simples en la proposición compuesta. Para construir todas las combinaciones posibles de valores de verdad de las proposiciones simples, en la primera columna se alternan los valores de verdad V y F en cantidad de 2^{n-1} cada uno. En la segunda columna, se alternan en cantidad de 2^{n-2}, y así sucesivamente, hasta llegar a la última columna en que se alternan en cantidad de 2^0.

Ejemplo 1

La tabla de verdad de $p \vee \neg p$ es

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

Ejemplo 2

La tabla de verdad de $(p \wedge q) \to q$ es

p	q	$p \wedge q$	$(p \wedge q) \to q$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

Ejemplo 3

La tabla de verdad de $\neg(p \to q) \leftrightarrow (p \wedge \neg q)$ es

p	q	$\neg q$	$p \to q$	$\neg(p \to q)$	$(p \wedge \neg q)$	$\neg(p \to q) \leftrightarrow (p \wedge \neg q)$
V	V	F	V	F	F	V
V	F	V	F	V	V	V
F	V	F	V	F	F	V
F	F	V	V	F	F	V

Ejemplo 4

La tabla de verdad de $(p \to q) \leftrightarrow \neg(\neg p \vee q)$ es

p	q	$\neg p$	$(p \to q)$	$(\neg p \vee q)$	$\neg(\neg p \vee q)$	$(p \to q) \leftrightarrow \neg(\neg p \vee q)$
V	V	F	V	V	F	F
V	F	F	F	F	V	F
F	V	V	V	V	F	F
F	F	V	V	V	F	F

Ejemplo 5

La tabla de verdad de $(p \to q) \wedge (\neg r \veebar q)$ es

p	q	r	$\neg r$	$(p \to q)$	$(\neg r \veebar q)$	$(p \to q) \wedge (\neg r \veebar q)$
V	V	V	F	V	V	V
V	V	F	V	V	F	F
V	F	V	F	F	F	F
V	F	F	V	F	V	F
F	V	V	F	V	V	V
F	V	F	V	V	F	F
F	F	V	F	V	F	F
F	F	F	V	V	V	V

Tautología: es una proposición compuesta que siempre es verdadera, independientemente de los valores de verdad de las proposiciones simples que la forman. Los ejemplos 1, 2 y 3 son tautologías.
Contradicción: es una proposición compuesta que siempre es falsa, independientemente de los valores de verdad de las proposiciones simples que la forman. El ejemplo 4 es una contradicción.
Utilizaremos el símbolo T para representar una tautología cualquiera y F para denotar una contradicción cualquiera.
Contingencia: es una proposición compuesta que no es tautología ni contradicción. El ejemplo 5 es una contingencia.

Consistente: es una proposición compuesta que es verdadera para por lo menos una combinación de los valores de verdad de las proposiciones simples que la componen. Es evidente que las

contingencias son consistentes, pero las proposiciones consistentes no necesariamente son contingencias. Las tautologías son consistentes y no son contingencias.

Proposiciones lógicamente equivalentes: dos proposiciones compuestas son lógicamente equivalentes , cuando tienen el mismo valor de verdad para todas las posibles combinaciones de los valores de verdad de las proposiciones simples que la componen. Es decir, cuando tienen la misma tabla de verdad.

Ejemplos

Cálculo proposicional

Consideremos las siguentes proposiciones. Construyamos algunas proposiciones compuestas.

p: "El frio llegó".
q: "El viento no sopla".
r: "Luis está de vacaciones".

Entonces las proposiciónes:

1. "El frio llegó y El viento no sopla", se escribe simbólicamente $p \wedge q$.
2. "Luis no está de vacaciones o El viento no sopla", se escribe $\neg r \vee q$.
3. "Es falso que (El frio llegó o El viento sopla)", se escribe $\neg(p \vee \neg q)$.

4. “El frio llegó, El viento sopla y Luis está de vacaciones”, se escribe $p \wedge \neg q \wedge r$.
5. “(El frio llegó y El viento no sopla) o (El frio no llegó y Luis no está de vacaciones)”, se escribe $(p \wedge q) \vee (\neg p \wedge \neg r)$.
6. “Si El frio llegó, entonces El viento no sopla”, se escribe $p \rightarrow q$.
7. “El frio llegó si y sólo si El viento no sopla”, se escribe $p \leftrightarrow q$.
8. “No es cierto que EL frio llegó si y sólo si El viento no sopla”, se escribe $\neg(p \leftrightarrow q)$.
9. “Luis no está de vacaciones si y sólo si El frio no llegó”, se escribe $\neg r \leftrightarrow \neg p$.

10. “Si El frio no llegó o El viento no sopla, entonces El frio llegó y El viento no sopla”, se escribe $(\neg p \vee q) \rightarrow (p \wedge q)$.

Ejemplos

Proposiciones simbólicas escritas en lenguaje natural, utilizando p, q y r anteriores :

$p \vee (q \vee r)$: “EL frio llegó o el viento no sopla o Luis está de vacaciones”.

$\neg p \wedge r$: “El frio no llegó y Luis está de vacaciones”.

$(\neg p \vee \neg r) \wedge \neg q$	:	"(El frio no llegó o Luis no está de vacaciones) y El viento sopla".
$\neg(p \wedge r)$	:	"No es cierto que (El frio llegó y Luis está de vacaciones)".
$(p \wedge \neg q) \vee \neg r$	:	"(El frio llegó y El viento sopla) o Luis no está de vacaciones".

$p \to r$	:	"Si El frio llegó, entonces Luis está de vacaciones".
$\neg r \leftrightarrow \neg p$	:	"Luis no está de vacaciones si y sólo si El frio no llegó".
$(p \to q) \vee (q \to p)$	:	"Si El frio llegó, entonces El viento no sopla o si El viento no sopla, entonces EL frio llegó".

Ejercicios 1

1. Suponga que p es una proposición falsa, q una proposición verdadera y r, una proposición falsa. De termine el valor de verdad de las siguientes proposiciones:

a.	$\neg p \vee q$	b.	$\neg(\neg p)$
c.	$\neg(p \wedge \neg q)$	d.	$\neg p \wedge \neg(\neg q)$
e.	$\neg\{(p \wedge q) \vee (\neg p \vee q)\}$	f.	$\neg(p \vee q) \wedge r$
g.	$\neg\{(p \vee q) \wedge r\}$	h.	$\neg p \wedge (q \wedge \neg r)$
i.	$(p \vee q \vee r) \leftrightarrow (p \wedge q \wedge r)$	j.	$(p \wedge q) \leftrightarrow p$

2. Considere las proposiciones:

p : El pavo es un cuadrúpedo.
q : Perú es un país africano.
r : La yuca es un tubérculo.

Determine el valor de verdad de las proposiciones siguientes:

a. $p \wedge \neg q$

b. $q \wedge r$

c $\neg(p \vee q) \wedge \neg(p \vee r)$

d. $\{p \rightarrow (q \rightarrow r)\} \leftrightarrow \{(p \rightarrow q) \rightarrow (p \rightarrow r)\}$

3. Construya la tabla de verdad de las siguientes proposiciones y determine cuáles son tautologías, contradicciones y contingencias:

a. $(p \wedge q) \rightarrow \neg q$

b. $\neg(p \vee q) \rightarrow p$

c. $\{p \vee (p \wedge q)\} \leftrightarrow p$

d. $p \wedge (p \vee q) \leftrightarrow p$

e. $(\neg p \vee q) \leftrightarrow (q \rightarrow p)$

f. $(q \wedge \neg p) \leftrightarrow (\neg q \vee p)$

g. $\{(p \vee q) \vee \neg r\} \rightarrow p$

h. $p \rightarrow \{(p \wedge q) \wedge \neg r\}$

i. $\neg(p \rightarrow q) \rightarrow (p \vee q)$

j. $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg q)$

k. $\{(p \wedge (p \rightarrow q)\} \rightarrow p$

l. $\{p \wedge (p \rightarrow q)\} \rightarrow q$

m. $(\neg p \vee q) \leftrightarrow (p \rightarrow q)$

n. $(p \wedge q) \leftrightarrow q$

4. Pruebe las siguientes tautologías de uso común (reglas de inferencia).

1.	$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$	De D'Morgan (DDM)
2.	$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$	De D'Morgan (DDM)
3.	$(p \vee q) \leftrightarrow (q \vee p)$	Conmutatividad (CONM)
4.	$(p \wedge q) \leftrightarrow (q \wedge p)$	Conmutatividad (CONM)
5.	$\neg\neg p \leftrightarrow p$	Doble negación (DN)
6.	$(p \rightarrow q) \leftrightarrow (\neg p \vee q)$	Def. condicional (DEF)
7.	$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$	Def. bicondicional (DEF)
8.	$(p \leftrightarrow q) \leftrightarrow [(p \wedge q) \vee (\neg p \wedge \neg q)]$	Def. bicondicional (DEF)
9.	$[(p \rightarrow q) \wedge p] \rightarrow q$	Modus Ponens (MP)
10.	$[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$	Modus Tollens (MT)

11.	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Transitividad (T)
12.	$(p \vee q) \wedge \neg p \to q$	Silogismo disy. (SD)
13.	$[(p \to q) \wedge (r \to s) \wedge (p \vee r)] \to (q \vee s)$	Dilema const. (DC)
14.	$[(p \to q) \wedge (r \to s) \wedge (\neg q \vee \neg s)] \to (\neg p \vee \neg r)$	Dilema dest. (DD)
15.	$(p \wedge q) \to p$	Simplificación (SIMP)
16.	$p \to (p \vee q)$	Adición (AD)
17.	$p \leftrightarrow (p \vee p)$	Tautología (TAU)
18.	$[p \vee (q \vee r)] \leftrightarrow [(p \vee q) \vee r]$	Asociatividad (ASOC)

19. $[p \wedge (q \wedge r)] \leftrightarrow [(p \wedge q) \wedge r]$ Asociatividad (ASOC)
20. $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ Transposición (TRANSP)
21. $[(p \wedge q) \rightarrow r] \leftrightarrow [p \rightarrow (q \rightarrow r)]$ Exportación (EXP)
22. $[p \wedge (q \vee r)] \leftrightarrow [(p \wedge q) \vee (p \wedge r)]$ Distribución (DIST)
23. $[p \vee (q \wedge r)] \leftrightarrow [(p \vee q) \wedge (p \vee r)]$ Distribución (DIST)
24. $(p \wedge q) \rightarrow (p \wedge q)$ Conjunción (CONJ)
25. $(p \wedge p) \leftrightarrow p$ Idempotencia (IDEM)
26. $(p \vee p) \leftrightarrow p$ Idempotencia (IDEM)
27. $(p \vee F) \leftrightarrow p$ Identidad (IDEN)
28. $(p \wedge T) \leftrightarrow p$ Identidad (IDEN)

29. $(p \vee T) \leftrightarrow T$ — Dominación (DOM)
30. $(p \wedge F) \leftrightarrow F$ — Dominación (DOM)
31. $[p \vee (p \wedge q)] \leftrightarrow p$ — Absorción (ABS)
32. $[p \wedge (p \vee q)] \leftrightarrow p$ — Absorción (ABS)
33. $(p \vee \neg p) \leftrightarrow T$ — Inversa (INV)
34. $(p \wedge \neg p) \leftrightarrow F$ — Inversa (INV)

5. Aplique la distribución a los enunciados siguientes
   a. $p \wedge (q \vee \neg s)$
   b. $r \vee (\neg p \wedge \neg q)$
   c. $s \wedge (t \vee \neg p)$

d. $(r \wedge s) \vee (q \wedge \neg r)$

e. $(r \vee s) \vee (q \wedge \neg r)$

f. $(r \wedge \neg s) \wedge (p \vee q)$

g. $[(p \vee q) \wedge (r \vee s)] \vee \neg p \vee \neg q$

h. $(p \wedge \neg q) \vee (r \wedge \neg s) \vee t \vee (q \wedge \neg r)$

6. Convierta las siguientes proposiciones en condicionales y después aplíquele la transposición (literal y simbólicamente).
   a. O hace frío o voy de paseo.
   b. Es falso que Lima sea la capital del Perú y Madrid no sea la capital de España.
   c. Pizarro conquistó el Perú y Cortés conquistó México

d. Es falso que Alberto sea médico o ingeniero

e. Es falso que Luis no tenga 25 años y Carlos no tenga 27 años.

Formas argumentales

En muchos casos se puede determinar, si un razomamiento es correcto o no en base a experiencias vividas. Sin embargo, en otros casos, decidir si un razonamiento es correcto o no, puede resultar muy complejo. Por tanto, se requiere de una mayor precisión para determinar cuando el razonamiento es correcto.

Una **forma argumental** es una proposición de la forma

$$(p_1 \wedge p_2 \wedge p_3 \wedge \ldots \wedge p_n) \Longrightarrow q$$

o

$$p_1,\, p_2,\, p_3,\, \ldots,\, p_n \vdash q,$$

donde p_1, p_2, p_3,...,p_n y q son proposiciones.
Es decir, una forma argumental es la representación simbólica de un razonamiento.

A las proposiciones

$$p_1,\, p_2,\, p_3,\, \ldots,\, p_n$$

se les llama **premisas o hipótesis** de la forma argumental y a la proposición q, se le llama **conclusión**.

Una forma argumental es **válida** si y sólo si, se obtiene la conclusión, a partir de las premisas dadas previamente.

Es decir, si es una tautología. En caso contrario, es una **falacia.**

Las tablas de verdad son instrumentos de fácil manejo y muy poderosos para probar la validez de razonamientos, sin embargo, no son prácticas cuando el número de proposiciones simples aumenta, ya que el número de filas de la tabla aumenta exponencialmente.

Esto hace que se utilicen procedimientos más prácticos en la prueba de validez de razonamientos, aunque se requiera de mayor capacidad de abstracción. Uno de estos procedimientos es el de la deducción proposicional.

Deducción proposicional

Las tautologías que fueron probadas en el ejercicio 4 se utilizan como reglas de inferencias para permitirnos inferir lógicamente de un conjunto de afirmaciones, otra afirmación.
Es importante señalar que la conclusión debe deducirse del conjunto de premisas aunque no sea directamente. Las premisas son proposiciones que se consideran siempre verdaderas.

Los pasos que se dan en la prueba de validez de un razonamiento deben estar siempre justificado por alguna de las reglas de inferencias. Cabe decir que este procedimiento sólo nos permite probar la validez de razonamientos y el hecho de que no lo hayamos probado, no quiere decir que no se pueda; simplemente que no hemos encontrado la solución.

Fórmulas proposicionales

Una **Fórmula proposicional** se define recursivamente de la siguiente manera:

a. Una variable proposicional es una fórmula proposicional.

b. Las proposiciones construidas de fórmulas proposicionales mediante las conectivas: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ y los símbolos auxiliares "(", ")"; "[","]" y "{", "}" son fórmulas proposicionales.

Nota. Cuando no haya lugar a confusión, utilizaré la palabra fórmula en lugar de fórmula proposicional.

Para **demostrar (probar) la validez de una forma argumental por deducción proposicional**, los pasos aceptados como válidos son:

1. En cualquier paso puede ser usado una premisa.

2. Todo paso puede ser sustituido por otro equivalente.

3. En todo paso se puede escribir la conclusión de una regla de inferencia, si sus premisas son pasos previos.

4. Cualquier teorema o propiedad conocida (reglas de inferencias) puede ser usada en un paso.

Ejemplos

Probar los siguientes razonamientos mediante deducción proposicional.

1. $p,\ \neg p \vee q,\ \neg r \rightarrow \neg q \vdash r$

   Prueba:

1)	p	P
2)	$\neg p \vee q$	P
3)	$\neg r \rightarrow \neg q$	P
4)	q	de 1) y 2) x SD
5)	$\neg\neg r$	de 3) y 4) x MT
6)	r	de 5) x DN

2. $t \to s,\ \neg q \to \neg s,\ t \vdash q$

Prueba:

1)	$t \to s$	P
2)	$\neg q \to \neg s$	P
3)	t	P
4)	s	de 1) y 3) x MP
5)	$\neg\neg q$	de 2) y 4) x MT
6)	q	de 5) x DN

3. $p \to q,\ q \to \neg r,\ r \vdash \neg p$

Prueba:

1)	$p \to q$	P
2)	$q \to \neg r$	P
3)	r	P
4)	$p \to \neg r$	de 1) y 2) x T
5)	$\neg p$	de 3) y 4) x MT

4. $(p \vee q) \to (r \wedge s),\ s \to t,\ \neg t \vdash \neg p$

Prueba:

1)	$(p \vee q) \to (r \wedge s)$	P
2)	$s \to t$	P
3)	$\neg t$	P
4)	$\neg s$	de 2) y 3) x MT
5)	$\neg s \vee \neg r$	de 4) x AD
6)	$\neg r \vee \neg s$	de 5) x CONM

Prueba (cont.)

7)	$\neg(r \wedge s)$	de 6) x DDM
8)	$\neg(p \vee q)$	de 1) y 7) x MT
9)	$\neg p \wedge \neg q$	de 8) x DDM
10)	$\neg p$	de 9) x SIMP

Pruebe la validez de los siguientes razonamientos mediante la deducción proposicional.

1. Juan no dice la verdad, o Pedro estuvo en casa cerca de las ocho. Si Pedro estuvo en casa cerca de las ocho, el vio a su hermano. Si Pedro vio a su hermano, sabe quien estuvo antes. Luego, si Juan dice la verdad, entonces Pedro sabe quien estuvo antes.

Solución

Consideremos las formas proposicionales:

p : Juan dice la verdad

q : Pedro estuvo en casa a las ocho

r : Pedro vio a su hermano

s : Pedro sabe quien estuvo antes

El razonamiento o forma argumental viene dado por:

$\neg p \vee q,\ q \to r,\ r \to s \vdash p \to s$

Prueba:

1)	$\neg p \vee q$	P
2)	$q \to r$	P
3)	$r \to s$	P
4)	$q \to s$	de 2) y 3) x T
5)	$p \to q$	de 1) x DEF
6)	$p \to s$	de 4) y 5) x T

2. No es cierto que Josefa esté con Rosa y Mayra. Si Hoy es Lunes, entonces Josefa está con Rosa. Hoy es Lunes. Luego, Josefa no está con Mayra.

Solución

Consideremos las formas proposicionales:
p : Josefa está con Rosa
q : Josefa está con Mayra
r : Hoy es Lunes

El razonamiento o forma argumental viene dado por:

$\neg(p \wedge q),\ r \rightarrow p,\ r\ \vdash \neg q$

Prueba:

1)	$\neg(p \wedge q)$	P
2)	$r \rightarrow p$	P
3)	r	P
4)	p	de 2) y 3) x MP
5)	$\neg p \vee \neg q$	de 1) x DDM
6)	$\neg q$	de 4) y 5) x SD

3. Si Felipe es constructor de apartamentos y Ángel compró un apartamento, entonces Antonio ganará la causa. Antonio no ganará la causa o Ángel es responsable. Pero Ángel no es responsable. Por tanto, Felipe no es constructor de apartamentos o Ángel no compró un apartamento

Solución

Consideremos las formas proposicionales:

p : Felipe es constructor de apartamentos

q : Ángel compró un apartamento

r : Antonio ganará la causa

s : Ángel es responsable

El razonamiento o forma argumental viene dado por:

$(p \wedge q) \rightarrow r,\ \neg r \vee s,\ \neg s\ \vdash \neg p \vee \neg q$

Prueba:

1)	$(p \wedge q) \rightarrow r$	P
2)	$\neg r \vee s$	P
3)	$\neg s$	P
4)	$\neg r$	de 2) y 3) x SD
5)	$\neg(p \wedge q)$	de 1) y 4) x MT
6)	$\neg p \vee \neg q$	de 5) x DDM

Ejercicios

Pruebe los siguientes razonamientos mediante deducción proposicional.

1. $p \leftrightarrow q,\ q \rightarrow \neg r,\ p \vdash \neg r$
2. $(t \wedge s) \leftrightarrow \neg r,\ r,\ t \vdash \neg s$
3. $r \vee s,\ \neg p,\ q \vee \neg r,\ p \leftrightarrow q \vdash s$
4. $\neg(p \wedge q),\ \neg q \rightarrow t,\ \neg p \rightarrow t,\ s \rightarrow \neg t \vdash \neg s$
5. $q \rightarrow t,\ \neg t \vee r,\ \neg r \vdash \neg q$
6. $(p \rightarrow q) \wedge (r \rightarrow s),\ (q \wedge s) \leftrightarrow t,\ \neg t \vdash (\neg p \vee \neg r)$
7. $(p \wedge q) \rightarrow r,\ \neg r \wedge p \vdash \neg q$
8. $(p \rightarrow q) \wedge (r \rightarrow s),\ p \vee r,\ (p \rightarrow \neg s) \wedge (r \rightarrow \neg q) \vdash (q \leftrightarrow \neg s)$

9. $p \to \neg q,\ r \to q,\ \neg r \to s,\ \neg p \to \neg t,\ \neg t \to \neg r,\ p \vee \neg p \vdash s$
10. $p \to q,\ q \to \neg r,\ s \vee r \vdash \neg p \vee s$
11. $(p \wedge q) \to r,\ (q \to r) \to s,\ p \vdash s$
12. $\neg p,\ \neg q \to \neg r,\ q \leftrightarrow p,\ t \to r \vdash \neg t$
13. $s \to p,\ \neg p \wedge \neg t,\ \neg t \to r \vdash \neg s \wedge r$
14. $p,\ p \to q,\ p \to (q \to r) \vdash r$
15. $p \to (q \to r),\ p,\ \neg r \vdash \neg q$
16. $\neg p \to q,\ \neg q \vdash p$
17. $(p \wedge \neg q) \to r,\ \neg r,\ p \vdash q$
18. $p \to (q \to r),\ p,\ \neg r \vdash \neg q$

19. $p \leftrightarrow q, p \vee q \vdash p \wedge q$

Pruebe la validez de los siguientes razonamientos mediante la deducción proposicional.

20. Si aumentan los precios, entonces aumenta la canasta familiar básica. Si aumenta la canasta familiar básica, entonces disminuye el poder adquisitivo del peso dominicano. Aumentan los precios. Luego, disminuye el poder adquisitivo del peso dominicano.
21. Si contratan a Juan para desarrollar un sistema y lo desarrolla bien, entonces le pagan buen sueldo. Contratan A juan para desarrollar un sistema y lo desarrolla bien. Por tanto,le pagan buen sueldo.

Ejercicios

22. Carlos es elegido si y sólo si la votación es numerosa. La votación es numerosa. Carlos no es elegido o Daniel será nombrado. Por tanto, Daniel será nombrado.
23. Si no hay subsidio del gobierno para la agricultura, entonces hay controles gubernativos sobre la agricultura. Si hay controles gubernativos sobre la agricultura, entonces no hay depresión agrícola. Hay depresión o superproducción agrícolas. Es un hecho que no hay sobreproducción. Entonces hay subsidios del gobierno para la agricultura.
24. El director no estudió bien la moción o la aprueba. Estudió todo muy bien, de modo que debe aprobar la moción.

Ejercicios

25. Habiendo tenido la víctima dinero en el bolsillo, el robo no fue el motivo del crimen. Pero el motivo del crimen fue el robo o la venganza. Luego, el motivo del crimen fue la venganza.
26. Si Luis viaja a New york, encontrará a Pedro. Si encuentra a Pedro, Luis recibirá la noticia. Luego, Luis recibe la noticia o no viaja a New york.
27. Carlos es Economista o médico. Pero si Carlos es economista, Carlos dominaría las matemáticas. Como no domina las matemáticas hay que inferir que Carlos es médico.

Ejercicios

28. Es falso que María y Rosa sean buenas programadoras. Si Rosa no es buena programadora, es rechazada para el trabajo. De la misma forma, si María no es buena programadora, es rechazada para el trabajo. Si Lily es buena programadora, no es rechazada para el trabajo. Por tanto, Lily no es buena programadora.

29. Si Juan es ingeniero de sistemas, es programador. Pero no es programador o es soporte técnico. No es soporte técnico. Por tanto, no es ingeniero de sistemas.

30. Si Arturo se casa, entonces María se enferma. María se enferma siempre y cuando Arturo no se haga sacerdote. Por tanto, si Arturo se casa, entonces no se hace sacerdote.

31. Tanto Juan como Pedro son matemáticos. Como Juan es matemático se tiene que si Pedro es matemático, entonces Luis es físico. Por tanto, Luis es físico.

32. Si un 1GB de memoria es mejor que nada, compraré más memoria. Como un 1GB de memoria es mejor que nada, compraré un nuevo computador. Por tanto, si un 1GB de memoria es mejor que nada, entonces compraré un nuevo computador y más memoria.

33. Considere las siguientes formas proposicionales:
    p : El dia está soleado.
    q : Hace calor.
    r : Luis está contento.

Ejercicios

Exprese verbalmente los razonamientos siguientes y pruebe la validez de los mismos:

a. $p \wedge q,\ p \rightarrow r \vdash\ r \wedge q$

b. $p \vee q,\ p \rightarrow r \vdash\ r \vee q$

c. $p \rightarrow (q \vee r),\ \neg q \wedge \neg r \vdash\ \neg p$

d. $p \rightarrow (q \rightarrow r),\ p \rightarrow q,\ p\ \vdash r$

e. $(p \wedge q) \rightarrow r,\ \neg r \wedge p\ \vdash\ \neg q$

Contenido

El procedimiento de la deducción proposicional tiene la limitación de que sólo nos permite probar la validez de un razonamiento, pero no la invalidez. Esto sin embargo, no significa que un procedimiento que no hayamos podido probar su validez sea inválido, sencillamente no lo hemos podido lograr.

Para vencer la limitación de la deducción proposicional surgen las llamadas formas normales.

Literal: Es una variable proposicional, negada o no negada.

Forma normal: es una fórmula proposicional formada sólo por conjunciones, disyunciones, y negaciones que afecten a una sola variable proposicional.

Las formas normales pueden ser:

- Forma normal disyuntiva (FND)

- Forma normal conjuntiva (FNC)

Forma normal disyuntiva (FND): es una fórmula proposicional F constituida por una disyunción finita de conjunciones finitas puras. Conjunciones finitas puras son aquellas cuyos componentes están formados por una sola variable proposicional negada o no negada (literal). Es decir,

$$\bigvee_{i=1}^{n}\left(\bigwedge_{j=1}^{m_i} L_{ij}\right),$$

donde cada L_{ij} es un literal.

Por ejemplo,

$$(p \wedge \neg q) \vee (\neg r \wedge \neg p \wedge \neg q) \vee (r \wedge \neg p \wedge q)$$

es una forma normal disyuntiva.

A las conjunciones finitas puras de la forma normal disyuntiva se les llama **sumandos**.

Forma normal conjuntiva (FNC): es una fórmula F constituida por una conjunción finita de disyunciones finitas puras. Disyunciones

finitas puras son aquellas cuyas componentes están formados por una sola variable proposicional negada o no negada (literal). Es decir,

$$\bigwedge_{i=1}^{n}\left(\bigvee_{j=1}^{m_i} L_{ij}\right),$$

donde cada L_{ij} es un literal.
Por ejemplo,

$$(\neg p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r) \wedge (r \vee \neg t \vee \neg r),$$

es una forma normal conjuntiva.

A las disyunciones finitas puras de la forma normal conjuntiva se les llama **factores**.

Para hallar cualquiera de las formas normales de una fórmula, el procedimiento que se sigue es el siguiente:

1. Eliminar todo lo que no sea conjunción o disyunción mediante las equivalencias

$$(p \to q) \Leftrightarrow (\neg p \vee q) \text{ y } (p \leftrightarrow q) \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q).$$

2. Eliminar las negaciones que afecten a los operadores o conectivas lógicas mediante las leyes de D'Morgan.
3. Aplicar las leyes de distribución, si se necesita.

Definición

El **Dual** de una proposición p que contiene solamente $\neg$, $\wedge$ y $\vee$, representado por p^d, se obtiene al sustituir cada ocurrencia de $\wedge(\vee)$ de p por $\vee(\wedge)$ y cada ocurrencia de $T(F)$ por $F(T)$.

Por ejemplo, las leyes de D'Morgan , así como también las leyes inversas son duales.

Principio de dualidad

Sean p y q proposiciones que sólo contienen $\neg$, $\wedge$ y $\vee$. Si p y q son lógicamente equivalentes, entonces p^d y q^d son lógicamente equivalentes.

Es decir, si $p \Leftrightarrow q$ entonces $p^d \Leftrightarrow q^d$.

Formas normales

A una fórmula constituida por $p \vee \neg p$ (afirmación o negación de una variable) se le llama **tercio excluido.** Observe que es una tautología. Una fórmula constituida por $p \wedge \neg p$ (afirmación y negación de una variable al mismo tiempo) se le llama **contradicción.**
La forma normal disyuntiva (FND) nos permite determinar si un razonamiento dado es **consistente o contradictorio.** Es **consistente** si al menos en un sumando no hay contradicción; en caso contrario, el razonamiento es **contradictorio.**

Ejemplo

Determine si el siguiente razonamiento es consistente mediante la FND:

$$[p \to (q \to r)] \to [(q \wedge p) \to r].$$

Solución:

$$
\begin{aligned}
[p \to (q \to r)] \to [(q \wedge p) \to r] &\Leftrightarrow \neg[p \to (q \to r)] \vee [(q \wedge p) \to r] \\
&\Leftrightarrow \neg[\neg p \vee (q \to r)] \vee [\neg(q \wedge p) \vee r] \\
&\Leftrightarrow [p \wedge \neg(\neg q \vee r)] \vee [(\neg q \vee \neg p) \vee r] \\
&\Leftrightarrow [p \wedge (q \wedge \neg r)] \vee [\neg q \vee \neg p \vee r] \\
&\Leftrightarrow (p \wedge q \wedge \neg r) \vee \neg q \vee \neg p \vee r
\end{aligned}
$$

Como no hay contradicción en al menos uno de los sumandos, se tiene que el razonamiento es consistente.

Ejemplo

Determine si el siguiente razonamiento es consistente mediante la FND:

$$[(p \to (q \wedge r)) \wedge (s \vee t)] \to [(p \vee r) \wedge (\neg q \vee \neg p)].$$

Solución:

$[(p \to (q \wedge r)) \wedge (s \vee t)] \to [(p \vee r) \wedge (\neg q \vee \neg p)] \quad \Leftrightarrow$

$\neg[(p \to (q \wedge r)) \wedge (s \vee t)] \vee [(p \vee r) \wedge (\neg q \vee \neg p)] \quad \Leftrightarrow$

$\neg[(\neg p \vee (q \wedge r)) \wedge (s \vee t)] \vee [(p \vee r) \wedge (\neg q \vee \neg p)] \quad \Leftrightarrow$

$[\neg(\neg p \vee (q \wedge r)) \vee \neg(s \vee t)] \vee [(p \vee r) \wedge (\neg q \vee \neg p)] \quad \Leftrightarrow$

$[(p \wedge \neg(q \wedge r)) \vee \neg(s \vee t)] \vee [(p \vee r) \wedge (\neg q \vee \neg p)] \quad \Leftrightarrow$

$[(p \wedge (\neg q \vee \neg r)) \vee (\neg s \wedge \neg t)] \vee [(p \vee r) \wedge (\neg q \vee \neg p)] \quad \Leftrightarrow$

$$[(p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg s \wedge \neg t)] \vee [((p \vee r) \wedge \neg q) \vee ((p \vee r) \wedge \neg p)] \quad \Leftrightarrow$$

$$[(p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg s \wedge \neg t)] \vee$$

$$[((p \wedge \neg q) \vee (r \wedge \neg q)) \vee ((p \wedge \neg p) \vee (r \wedge \neg p))] \quad \Leftrightarrow$$

$$(p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg s \wedge \neg t) \vee$$

$$(p \wedge \neg q) \vee (r \wedge \neg q) \vee (p \wedge \neg p) \vee (r \wedge \neg p) \quad \Leftrightarrow$$

$$(p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg s \wedge \neg t) \vee (r \wedge \neg q) \vee (p \wedge \neg p) \vee (r \wedge \neg p) \quad \text{FND}$$

Como no hay contradicción en al menos uno de los sumandos, se tiene que el razonamiento es consistente.

Determine si los siguientes razonamientos son consistentes, mediante la FND.

1. $(p \vee q) \leftrightarrow (\neg p \rightarrow q)$
2. $[(p \rightarrow r) \wedge (r \rightarrow q)] \rightarrow (p \rightarrow q)$
3. $(p \vee q) \leftrightarrow \neg(\neg p \wedge \neg q)$
4. $[(p \vee q) \rightarrow (\neg q \wedge s)] \rightarrow (\neg p \vee \neg q)$
5. $(q \rightarrow r) \rightarrow [(q \vee p) \rightarrow (r \vee p)]$
6. $[(p \vee (q \wedge r)) \wedge (\neg q \vee (r \wedge p))] \rightarrow p$
7. $[(p \vee r) \wedge \neg s] \rightarrow [s \wedge (\neg p \vee \neg r)]$
8. $[(p \wedge q) \vee r] \rightarrow [(s \wedge t) \wedge (\neg p \vee \neg q)]$

Ejercicios

9. $(p \to q) \to [(p \wedge r) \to (q \wedge r)]$

Con la forma normal conjuntiva (FNC) podemos determinar si un razonamiento es válido (tautología) o inválido. Una forma normal conjuntiva es tautológica, si en todos sus factores hay tercio excluido; en caso contrario es inválida.

Ejemplo

Determinar mediante la FNC si el siguiente razonamiento es válido o inválido.

$$(\neg p \wedge q) \rightarrow [(q \vee r) \rightarrow p]$$

Solución:

$$\begin{aligned}
(\neg p \wedge q) \to [(q \vee r) \to p] &\Leftrightarrow \neg(\neg p \wedge q) \vee [(q \vee r) \to p] \\
&\Leftrightarrow (p \vee \neg q) \vee [(q \vee r) \to p] \\
&\Leftrightarrow (p \vee \neg q) \vee [\neg(q \vee r) \vee p] \\
&\Leftrightarrow (p \vee \neg q) \vee [(\neg q \wedge \neg r) \vee p] \\
&\Leftrightarrow (p \vee \neg q) \vee p \vee (\neg q \wedge \neg r) \\
&\Leftrightarrow [(p \vee \neg q \vee p)] \vee (\neg q \wedge \neg r) \\
&\Leftrightarrow (p \vee \neg q \vee p \vee \neg q) \wedge (p \vee \neg q \vee p \vee \neg r) \\
&\Leftrightarrow (p \vee \neg q) \wedge (p \vee \neg q \vee \neg r)
\end{aligned}$$

Como no hay tercio excluido en todos los factores, el razonamiento (forma argumental) es inválido (falacia).

Ejemplo

Determinar mediante la FNC si el siguiente razonamiento es válido o inválido.

$$(p \wedge q) \rightarrow [(q \wedge r) \vee p]$$

Solución:

$$
\begin{aligned}
(p \wedge q) \rightarrow [(q \wedge r) \vee p] &\Leftrightarrow \neg(p \wedge q) \vee [(q \wedge r) \vee p] \\
&\Leftrightarrow (\neg p \vee \neg q) \vee [(q \wedge r) \vee p] \\
&\Leftrightarrow (\neg p \vee \neg q) \vee p \vee (q \wedge r) \\
&\Leftrightarrow (\neg p \vee \neg q \vee p) \vee (q \wedge r) \\
&\Leftrightarrow (\neg p \vee \neg q \vee p \vee q) \wedge (\neg p \vee \neg q \vee p \vee r)
\end{aligned}
$$

Como hay tercio excluido en todos los factores, el razonamiento es válido.

Ejercicios

Determine mediante la FNC si los siguientes razonamientos son válidos o inválidos

1. $\neg(p \vee q) \vee (p \to q)$
2. $[(p \to r) \wedge (r \to q)] \to (p \to q)$
3. $[(p \wedge q) \to (\neg p \wedge s)] \to (\neg q \wedge p)$
4. $[(p \to q) \wedge p] \to q$
5. $(p \to q) \to [(p \vee q) \to q]$
6. $[p \to (q \to r)] \to [(p \wedge q) \to r]$
7. $(p \vee q) \leftrightarrow (\neg p \to q)$
8. $(\neg p \to q) \to (\neg q \to p)$

9. $(p \to q) \to (r \vee s)$
10. $(q \to r) \to [(p \to q) \to (p \to r)]$

Contenido

Cuantificadores

Las herramientas lógicas que hemos visto hasta ahora no son suficientes como para expresar en lenguaje lógico todas las situaciones que se presentan en el lenguaje común. Los cuantificadores vienen a llenar este vacío porque permiten construir proposiciones particularizadas o generalizadas a partir de funciones proposicionales.

Un símbolo que puede representar a cualquier objeto de una colección dada de tales objetos se le llama **variable**.

Sea $P(x)$ una oración que depende de la variable x, donde los valores de x pertenecen a un conjunto D. P recibe el nombre de **función proposicional** o **predicado** sobre D, si para cada $x \in D$, $P(x)$ es una proposición. Es decir, si al sustituir x por un objeto cualquiera de D, P se convierte en una proposición. Al conjunto D se le llama **dominio de discurso** o **dominio de referencia** o **dominio de definición.**
Por ejemplo, sea

$$P(x) : x \text{ es un entero primo,}$$

donde $D = \mathbb{Z}^+$.

Puesto que $P(x)$ se convierte en una proposición para cada valor de x, ya que dependiendo de que x sea primo o no, $P(x)$ es verdadera o falsa. Entonces podemos decir que $P(x)$ es una función proposicional.

Ejemplos

Los siguientes enunciados son funciones proposicionales

a. $x^2 + 7x + 12 = 0$, donde $D = \mathbb{R}$

b. x es un entero divisible por 3, donde $D = \mathbb{Z}^+$

c. x es un beisbolista que dió 40 jonrones o más en la campaña del 2009 en GL. D = conjunto de beisbolistas

Sea $P(x)$ una función proposicional con dominio de referencia D . Las expresiones del lenguaje común como:
"Existe un x $P(x)$", "Para algún x $P(x)$", corresponden a afirmaciones cuantificadas existencialmente y se escriben como

$$\exists x \ P(x).$$

EL símbolo $\exists$ significa "existe" y representa el **cuantificador existencial.**
La expresión

$$\exists x \ P(x)$$

es **verdadera** si $P(x)$ es verdadera para al menos un $x \in D$ y **falsa** si $P(x)$ es falsa para toda $x \in D$.

Ejemplo

La afirmación

$$\exists x \ (2x + 3 = 10), \quad D = \mathbb{R}$$

es verdadera porque existe un número real $x = \dfrac{7}{2}$ para el cual la proposición es verdadera.
La afirmación

$$\exists x \ (x^2 + 1 = 0), \quad D = \mathbb{R}$$

es falsa porque no existe un número real para el cual la proposición sea verdadera.

Expresiones como “Para cualquier x $P(x)$”, “Para todo x $P(x)$” , “Para cada x $P(x)$” representan afirmaciones cuantificadas universalmente y

se escribe como $\forall x \ P(x)$. El símbolo $\forall$ significa “para todo” y representa el **cuantificador universal**.
La afirmación

$$\forall x \ P(x)$$

es **verdadera** si $P(x)$ es verdadera para cada $x \in D$ y **falsa** si $P(x)$ es falsa para al menos un $x \in D$.

Ejemplo

La afirmación

$$\forall x \ (x^2 + 1 > 0), \quad D = \mathbb{R}$$

es verdadera, porque $x^2 + 1 > 0$ es verdadera para cada $x \in D$.

La afirmación

$$\forall x \left(\frac{x}{x^2+1} = \frac{3}{10} \right), \quad D = \mathbb{R}$$

es falsa, porque

$$\frac{x}{x^2+1} = \frac{3}{10}$$

es falsa para por lo menos un $x \in D$, digamos para $x = 2$.

Equivalencia de cuantificadores

a. $\forall x \; P(x) \Leftrightarrow \neg \exists x \; \neg P(x)$

b. $\exists x \; P(x) \Leftrightarrow \neg \forall x \; \neg P(x)$

Leyes de De Morgan para lógica

a. $\neg(\forall x\ P(x)) \Leftrightarrow \exists x\ \neg P(x)$

b. $\neg(\exists x\ P(x)) \Leftrightarrow \forall x\ \neg P(x)$

Muchas veces las expresiones del lenguaje común tienen interpretaciones diferentes, por ejemplo la afirmación

"No todo entero primo es impar"

puede interpretarse como:

"Todo entero primo no es impar".

Esta no es la interpretación correcta.
La interpretación correcta es:

"Algún entero primo no es impar."

Consideremos las siguientes funciones proposicionales:
$P(x)$: x es entero primo
$Q(x)$: x es impar.
La primera interpretación se escribe como:

$$\forall x\ (P(x) \to \neg Q(x))$$

y la segunda se escribe

$$\exists x\ (P(x) \wedge \neg Q(x)).$$

Observe que

$$\exists x\ (P(x) \wedge \neg Q(x)) \Leftrightarrow \exists x\ \neg(P(x) \to Q(x)).$$

De la misma manera se observa que

$$\exists x\ \neg(P(x) \to Q(x)) \Leftrightarrow \neg(\forall x\ (P(x) \to Q(x))).$$

Para indicar expresiones como: “Existe un único”, “Hay un solo”, “Hay un único”, se utiliza otro cuantificador del cual no hemos hablado que es:

$$\exists!.$$

Cuando de escribe

$$\exists!\, x\, P(x),$$

se quiere decir que hay un único elemento x tal que $P(x)$.

La proposición

$$\exists!\, x\, P(x)$$

es **verdadera**, si y sólo si, existe un único objeto en el dominio de definición de x para el cual $P(x)$ es verdadera. Es **falsa** cuando $P(x)$ es falsa para todos los valores de x dentro de su dominio de definición o cuando hay más de un valor de x para los cuales $P(x)$ es verdadera.

Ejercicios

1. Determine si el enunciado dado es una función proposicional. Si lo es, encuentre el dominio de referencia.
   a. $7^n - 1$ es múltiplo de 6

b. Elija un entero entre 3 y 19

c. Los medias rojas de Boston ganaron la serie mundial del 2007

d. $3x - 5 = 2$

2. Considere la función proposicional:
$P(n)$: "3 divide a $(2n - 1)$, $\quad D = \mathbb{Z}^+$".

   Escriba cada proposición en palabras y diga el valor de verdad de las siguientes proposiciones:

   a. $P(4)$ **b.** $P(5)$ **c.** $P(8)$ **d.** $P(11)$ **e.** $\forall n\ P(n)$

3. Considere la función proposicional $P(x)$: "x es un golfista". El dominio de referencia es el conjunto de deportistas. Escriba en palabras cada proposición.

a. $\exists x \; P(x)$
b. $\forall x \; \neg P(x)$
c. $\exists x \; \neg P(x)$
d. $\neg(\forall x \; P(x))$

4. Escriba la negación de los ejercicios del punto 3 en símbolos y palabras.
5. Considere las funciones proposicionales: $P(x)$: "x es un profesor universitario" y $Q(x)$: "x enseña matemática". EL dominio de referencia es el conjunto de todos los profesores. Escriba en palabras y determine el valor de verdad de cada afirmación.

a. $\forall x \; (P(x) \rightarrow Q(x))$
b. $\forall x \; (P(x) \vee Q(x))$
c. $\exists x \; (Q(x) \rightarrow P(x))$

d. $\exists x\ (P(x) \wedge Q(x))$

6. Escriba la negación de los ejercicios del punto 5 en símbolos y palabras.
7. Considere las funciones proposicionales

   $P(x)$: "x es un abogado"

   $Q(x)$: "x tiene un yate".

   Escriba en símbolos y en palabras las siguientes afirmaciones.

   a. Todos los abogados tienen un yate
   b. Algunos abogados tienen un yate
   c. Todos los dueños de yate son abogados
   d. Alguien que tiene un yate es abogado

8. Escriba la negación en símbolos y palabras de los ejercicios del punto 7.
9. Determine el valor de verdad de cada afirmación. EL dominio de referencia es $\mathbb{R}$.
   a. $\forall x\ (x^2 > x)$
   b. $\exists x\ (x^2 > x)$
   c. $\forall x\ (x > 1 \rightarrow x^2 > x)$
   d. $\exists x\ (x > 1 \rightarrow x^2 > x)$
   e. $\forall x\ (x > 1 \rightarrow x/(x^2 + 1) < 1/3)$
10. Escriba la negación en símbolos y en palabras de los ejercicios del punto 9.

En el cálculo proposicional, las variables representan proposiciones atómicas. Es decir, aquella en la que una propiedad determinada se le atribuye a un sujeto. Es claro que a un mismo sujeto se le puede atribuir distintas propiedades y una misma propiedad la pueden tener varios sujetos.
Por ejemplo, de Pedro se puede decir que es gordo, alto, inteligente. Del mismo modo, mamífero se le puede atribuir a una Vaca, un caballo, un Perro, etc.
El cálculo de predicados considera los diferentes elementos que intervienen en las proposiciones, mientras que en el cálculo proposicional, las proposiciones se consideran como un todo.
En el cálculo de predicados, llamamos **término** al sujeto del que se predica algo y **predicado**, lo que se dice del sujeto.

Los sujetos constantes, individuales o particulares se nombran generalmente con letras minúsculas como: a, b, c, etc., mientras que el símbolo x, se utiliza para variables de sujetos o individuos.

Consideremos el argumento:

Todos los caballos son cuadrúpedos. Santy es un caballo. Por tanto, Santy es un cuadrúpedo.
Sean
p : Todos los caballos son cuadrúpedos.
q : Santy es un caballo.
r : Santy es un cuadrúpedo.

La forma argumental de este argumento, viene dada por:

$$(p \wedge q) \rightarrow r.$$

Esta forma argumental no es válida, ya que la forma proposicional es una contingencia.
Sin embargo, desde el punto de vista lógico intuitivo, este argumento parece ser válido. Esto nos lleva a pensar que la lógica proposicional que hemos desarrollado hasta ahora no tiene las herramientas suficientes que nos permita establecer la relación entre las premisas y la conclusión.

El cálculo de predicados suple esta deficiencia.

Por ejemplo, tomemos la proposición:

“Todos lo matemáticos son científicos”
Podemos decir que si José es matemático, entonces José es científico. De la misma forma, si Pedro es matemático, entonces Pedro es científico. De modo más general, podemos escribir: si x es matemático, entonces x es científico. Consideremos la función proposicional:

$P(x)$: x es matemático $\to$ x es científico.
La expresión $\forall\, x\ P(x)$ se interpreta como: para todo x, si x es matemático, entonces x es científico. En lo adelante Cuando haya posibilidad de confusión en la notación, usaremos el símbolo “:” para separar el cuantificador de la función proposicional. Así escribiremos

$$\forall\, x\ :\ P(x).$$

En el caso del enunciado anterior, podemos escribir

$$\forall x \ : \ x \text{ es matemático } \rightarrow \ x \text{ es científico.}$$

Teorema

Si $P(x)$ es una función proposicional y a un objeto del dominio de definición de x, entonces

$$\forall x \, P(x) \rightarrow P(a)$$

es una tautología.

Demostración

Si suponemos que la condicional es falsa es porque $\forall x \, P(x)$ es verdadera y $P(a)$ es falsa. Ahora bien, si $P(a)$ es falsa, entonces

$\forall\, x\, P(x)$ es falsa y esto es contradictorio con el hecho de que $\forall\, x\, P(x)$ es verdadera.
Para probar la validez de argumentos que incluyen proposiciones universales se pueden aplicar las mismas reglas de inferencias (o de derivación) del cálculo proposicional. Tomemos como ejemplo el argumento:

Todos los santiagueros son cibaeños. Todos los cibaeños son emprendedores. Luego, todos los santiagueros son emprendedores.

Este argumento se escribe en forma simbólica como:
Sean
$P(x)$: x es santiaguero.
$Q(x)$: x es cibaeño.

$R(x)$: x es emprendedor.

Entonces el argumento lo escribimos como:

$\forall x : P(x) \rightarrow Q(x), \forall x : Q(x) \rightarrow R(x) \vdash \forall x : P(x) \rightarrow R(x)$

Prueba

Como las premisas son verdaderas, tomemos un objeto particular cualquiera del dominio de definición de x, digamos x_0 y hagamos

p : x_0 es santiaguero.
q : x_0 es cibaeño.
r : x_0 es emprendedor.

Entonces el argumento se escribe:

$p \to q,\ q \to r \ \vdash\ p \to r$
Es evidente que este argumento es válido, según la derivación del cálculo proposicional porque corresponde a la regla de inferencia de transitividad.

Consideremos el argumento:

Todos los caballos son cuadrúpedos. Santy es un caballo. Por tanto, Santy es un cuadrúpedo.
Sean
$P(x)$: x es un caballo.
$Q(x)$: x es un cuadrúpedo.
$P(x_0)$: Santy es un caballo.

Entonces el argumento se escribe como:

$\forall x : P(x) \to Q(x),\ P(x_0) \vdash Q(x_0)$

Prueba

Como las premisas son ambas verdaderas, se puede aplicar la regla de inferencia del Modus Ponens del cálculo proposicional y se obtiene la conclusión.

Ejercicios

Determine si los argumentos siguientes son válidos o no.

1. Todos los Físicos son analistas. Todos los analistas son inteligentes. Luego, todos los Físicos son inteligentes.
2. Toda persona cariñosa es amada. Todos los que son amados son dichosos. Juan es cariñoso. luego, Juan es dichoso.

3. Toda figura es un cuadrilátero. Un triángulo es una figura. Por tanto, un triángulo tiene cuatro lados.
4. Todos los beisbolistas son atletas. Todos los futbolistas son atletas. Por tanto, todos los beisbolistas son futbolistas.
5. Los guineos son frutas agradables y saludables. Toda fruta agradable y saludable no se desarrolla en pantanos. Luego, los guineos no se desarrollan en pantanos.
6. Todo el que ama es un enfermo. Pedro vive en la ciudad. Todo el que vive en la ciudad no ama. Por tanto, Pedro no es un enfermo.
7. Toda persona inteligente es estudiosa. Toda persona estudiosa es exitosa. Todo hombre es exitoso. Luego, Todo hombre es inteligente.

Consideremos el argumento:

Algunos hombres son inteligentes. Todas las personas inteligentes son sabias. Luego, Algunos hombres son sabios.

Sean
$P(x)$: x es un hombre.
$Q(x)$: x es inteligente.
$R(x)$: x es sabio.

El argumento en forma simbólica se escribe como:

$$\exists x \ : P(x) \wedge Q(x), \ \forall x \ : Q(x) \rightarrow R(x) \ \vdash \exists x \ : P(x) \wedge R(x)$$

Prueba

Como suponemos que las premisas son verdaderas, existe por lo menos un objeto x_0 en el dominio de definición de x para el cual la proposición es $P(x_0) \wedge Q(x_0)$ y por tanto, ambas son verdaderas. Como la segunda premisa es verdadera, se tiene que $Q(x_0) \to R(x_0)$ es verdadera. Ahora bien, como $Q(x_0)$ es verdadera, se tiene que $R(x_0)$ es verdadera. Luego, tenemos que $P(x_0) \wedge R(x_0)$ es verdadera y $\exists\, x\ : P(x) \wedge R(x)$ es una proposición verdadera. Luego, el argumento es válido.

Este argumento es un caso particular del argumento del cálculo prosicional

$$p \wedge q,\ q \to r\ \vdash p \wedge r,$$

que es un argumento válido.

Ejercicios

Determine si los argumentos siguientes son válidos o no.

1. Todos los filósofos son científicos. Algunos hombres son filósofos. Luego, hay hombres que son científicos.
2. Si un hombre toca guitarra, entonces es músico. Hay hombres que son músicos. Por tanto, hay hombres que tocan guitarra.
3. Algunos conductores son imprudentes. Los conductores imprudentes son agresivos. Luego, Algunos conductores imprudentes son agresivos.
4. Algunos seres vivos son parásitos. Los hombres son seres vivos. Por tanto, Algunos hombres son parásitos.

5. Los universitarios que estudian son exitosos. Hay universitarios que no estudian. Por tanto, Hay universitarios que no son exitosos.
6. Todos los músicos clásicos son artistas. Existen músicos que no son artistas. Luego, existen músicos que no son clásicos.

Cuantificadores anidados

Los cuantificadores anidados se utilizan cuando necesitamos dos o más variables en una función proposicional. Por ejemplo, cuando escribimos

$$\forall x \forall y (x^2 + y^2 \geq 0), \quad D = \mathbb{R},$$

queremos significar que para cada x y para cada y, se tiene que $(x^2 + y^2 \geq 0)$. Evidentemente que esta afirmación es verdadera.

Si se escribe

$$\forall x \exists y \ (x + y = 0), \quad D = \mathbb{R},$$

significamos que para cada x existe al menos una y tal que $x + y = 0$. Esta afirmación es verdadera.

Cuando se escribe

$$\forall x \exists y \ (x > y), \quad D = \mathbb{Z}^+,$$

queremos decir que para toda x, existe una y tal que $x > y$.

Esta afirmación es falsa porque existe al menos una x, digamos $x = 1$ para la cual $x > y$ es falsa para todo entero positivo y.

Consideremos la afirmación

$$\exists x \exists y((x < 0) \wedge (y < 0) \wedge (xy = 15)), \quad D = \mathbb{Z}^{-}.$$

Esto significa que existe una x y existe una y, digamos $x = -3$ y $y = -5$ tal que $xy = 15$, lo cual es verdadera.

Considere la afirmación

$$\exists x \forall y \ (x \geq y), \quad D = \mathbb{Z}^{+}.$$

Esta afirmación es falsa.

Negación de cuantificadores en dos variables

La negación de cuantificadores en dos variables se obtiene aplicando las leyes de D'Morgan repetidamente. De modo que

a. $\neg(\forall x \forall y\, P(x,y)) \Leftrightarrow \exists x \neg(\forall y\, P(x,y)) \Leftrightarrow \exists x\, \exists y\, \neg P(x,y)$

b. $\neg(\forall x \exists y\, P(x,y)) \Leftrightarrow \exists x \neg(\exists y\, P(x,y)) \Leftrightarrow \exists x\, \forall y\, \neg P(x,y)$

c. $\neg(\exists x \forall y\, P(x,y)) \Leftrightarrow \forall x \neg(\forall y\, P(x,y)) \Leftrightarrow \forall x\, \exists y\, \neg P(x,y)$

d. $\neg(\exists x \exists y\, P(x,y)) \Leftrightarrow \forall x \neg(\exists y\, P(x,y)) \Leftrightarrow \forall x\, \forall y\, \neg P(x,y)$

Ejercicios

1. Considere la función proposición $P(x, y)$: "$x \geq y$". EL dominio de referencia es $\mathbb{Z}^+$. Determine el valor de verdad de cada una de las siguientes proposiciones.
   a. $\forall x \forall y\ P(x, y)$
   b. $\exists x \forall y\ P(x, y)$
   c. $\exists x \exists y\ P(x, y)$
2. Escriba la negación de cada uno de los ejercicios del punto 1.
3. Determine el valor de verdad de las siguientes proposiciones. El dominio de referencia es $D = \mathbb{R}$.
   a. $\forall x \forall y\ (x^2 < y + 1)$
   b. $\exists x \forall y\ (x^2 < y + 1)$
   c. $\forall x \forall y\ (x^2 + y^2 = 9)$

d. $\forall x \forall y\ (x^2 + y^2 \geq 0)$
e. $\exists x \forall y\ (x^2 + y^2 = 9)$

f. $\forall x \forall y\ ((x < y) \rightarrow (x^2 < y^2))$
g. $\exists x \forall y\ ((x < y) \rightarrow (x^2 < y^2))$
h. $\exists x \exists y\ ((x < y) \rightarrow (x^2 < y^2))$
i. $\forall x \exists y\ (x^2 + y^2 = 9)$
j. $\forall y \exists x\ (x^2 < y + 1)$
k. $\forall x \exists y\ (x^2 + y^2 \geq 0)$
l. $\exists x \exists y\ (x^2 + y^2 \geq 0)$

4. Escriba la negación de cada uno de los ejercicios del punto 3.

Contenido

Contenido

Contenido

Contenido

Contenido

Contenido

Conjuntos

Un **conjunto** es cualquier colección de objetos bien definidos en el sentido de que se pueda determinar con precisión y sin ambiguedad cuando un objeto pertenece o no al conjunto. A los objetos que componenen un conjunto se les llama **elementos o miembros** del conjunto. Por ejemplo, el conjunto de las letras del alfabeto castellano; el conjunto de los numeros reales entre cero y uno, etc.. Los conjuntos representan la base sobre la cual se construye toda la matemática. De aquí su importancia en todo estudio científico.
Los conjuntos se representan generalmente por letras mayúsculas como $A, B, C, S, T, \dots$ y sus elementos, por letras minúsculas como $x, y, z, s, t, a, \dots$.

Para indicar que el objeto x es elemento o miembro del conjunto A, se escribe

$$x \in A$$

y para decir que x no pertenece al conjunto A se escribe

$$x \notin A$$

Los conjuntos se pueden describir por **extensión o comprensión.** Un conjunto se define por **extensión** cuando sus elementos se enlistan entre llaves, separados por comas.
Por ejemplo, el conjunto

$$\{a, b, c, d\},$$

está descrito por extensión. El orden de los elementos en un conjunto no tiene importancia.
De aquí que los conjuntos

$$\{d, c, b, a\},\ \{b, a, c, d\},\ \{c, a, d, b\},$$

representan todos, al conjunto dado.
En un conjunto los elementos no se repiten, es decir, los elementos repetidos, sencillamente se ignoran.
Un conjunto se describe por **comprensión** cuando se especifica una propiedad común que satisfacen los elementos del conjunto. Sea $P(x)$ una función proposicional referente al objeto x.
La forma de escribir el conjunto por comprensión es

$$\{x \mid P(x)\},$$

que significa la colección de todos los objetos x para los que P hace sentido y es verdadera.
Por ejemplo,

$$\{x \mid x \text{ es un entero positivo par menor que 10}\}$$

es el conjunto

$$\{2, 4, 6, 8\}.$$

En el primer caso, tenemos un conjunto definido por comprensión y luego, el mismo conjunto, pero definido por extensión.

Ejemplo

El conjunto de todas las letras de la palabra “bits” se puede describir como

$$\{\text{b, i, t, s}\}$$

o por

$$\{x \mid x \text{ es una letra en la palabra “bits”}\}.$$

El conjunto que no tiene elemento se le llama **conjunto vacío** y se representa por $\emptyset$ o $\{\ \}$.

Por ejemplo,

$$\emptyset = \{x \mid x \text{ es un número real y } x^2 + 1 = 0\},$$

puesto que el cuadrado de un número real es siempre mayor o igual a cero.

Subconjunto

Decimos que un conjunto A es **subconjunto** del conjunto B si todos los elementos de A son también elementos de B, es decir, si cuando $x \in A$, entonces $x \in B$ o

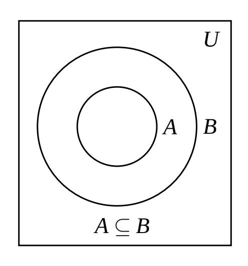
$$\forall x : [x \in A \rightarrow x \in B].$$

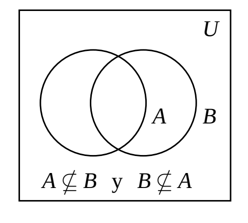
Se escribe

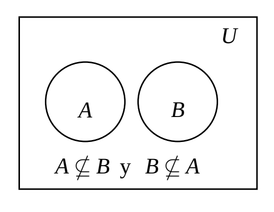
$$A \subseteq B.$$

Si un conjunto A no es subconjunto de B, se escribe

$$A \nsubseteq B.$$







Por ejemplo, sean

$$A = \{2, 4, 5\}, B = \{1, 2, 3, 4, 5, 6\}, D = \{3, 4, 5, 6, 7\}.$$

Se observa que $A \subseteq B$, $A \nsubseteq D$, $B \nsubseteq D$.

Las relaciones entre conjuntos pueden ser representadas mediante los llamados **diagramas de Venn** en honor al lógico John Venn. Así, Si A es un conjunto cualquiera, entonces $A \subseteq A$. Es decir, cualquier conjunto es subconjunto de si mismo.

Es fácil probar que $\emptyset \subseteq A$ para cualquier conjunto A.

Ejemplo

Consideremos un conjunto X y sea

$$T = \{X, \{X\}\}.$$

Es claro que $X \in T$ y $\{X\} \in T$. Luego, podemos decir que

$$\{X\} \subseteq T \text{ y } \{\{X\}\} \subseteq T.$$

Por otro lado, es evidente que $X \not\subseteq T$.

Notación

Para algunos conjuntos de uso común en este curso, usaremos la siguiente notación

a. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
b. $\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, \dots\}$
c. $\mathbb{Z}^{+} = \{1, 2, 3, \dots\}$
d. $\mathbb{Z}^{-} = \{\dots, -3, -2, -1\}$

Notación (cont.)

e. $\mathbb{Q} = \left\{ \frac{a}{b} \,|\, a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \neq 0 \right\}$

f. $\mathbb{I} = \left\{ x \,|\, x \text{ no se puede expresar como } \frac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z} \right\}$

g. $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$

h. $\mathbb{R}^* = \mathbb{R} \cup \{-\infty, +\infty\}$ = conjunto de los reales extendidos.

Igualdad

Decimos que los conjuntos A y B son **iguales**, si y sólo si, tienen exactamente los mismos elementos. Se escribe

$$A = B.$$

Por ejemplo, los conjuntos

$$A = \{x \,|\, x \text{ es un número entero y } x^2 - 1 = 0\} \text{ y } B = \{-1, 1\},$$

son iguales. Es decir,

$$A = B.$$

Es fácil probar que

$$A = B, \text{ si y sólo si, } A \subseteq B \text{ y } B \subseteq A.$$

Por ejemplo:

Consideremos los conjuntos

$$A = \{r \in \mathbb{Z} | r = 3m \text{ para algún entero } m\}$$

y

$$B = \{s \in \mathbb{Z} | s = 3n + 3 \text{ para algún entero } n\}.$$

Probemos que $A = B$.
Prueba:

Debemos probar que $A \subseteq B$ y $B \subseteq A$.

Primero. Probemos que $A \subseteq B$.

Sea $x \in A$, entonces existe un $m \in \mathbb{Z}$ tal que $x = 3m$. Ahora bien, podemos escribir $x = 3n + 3$ donde $n = m - 1$ es también un entero. Por tanto, $x \in B$ y $A \subseteq B$.

Segundo. Probemos que $B \subseteq A$.

Sea $x \in B$, entonces existe un $n \in \mathbb{Z}$ tal que $x = 3n + 3$. Ahora bien, podemos escribir $x = 3m$ donde $m = n + 1$ es también un entero. Por tanto, $x \in A$ y $B \subseteq A$. Luego, $A = B$. ■

El conjunto que contiene todos los elementos con los cuales se trabaja en el estudio se le llama **conjunto universo** o **conjunto universal** y se representa por U. Esto es, todos los conjuntos con los cuales trabajamos suponemos que son subconjuntos del conjunto universo. Cuando no haya lugar a confusión en el contexto de trabajo,

obviaremos el conjunto universo. Un conjunto A es **finito** si posee n elementos distintos, donde $n \in \mathbb{N}$. Al número n se le llama **cardinal** de A y lo representamos por $|A|$. Por ejemplo, los conjuntos

$$A = \{1, 2, 3, 4, 5\} \text{ y } B = \{x \in \mathbb{R} | x^2 - 1 = 0\}$$

son finitos y tienen como cardinales $|A| = 5$ y $|B| = 2$.

Los conjuntos $\mathbb{N}$ y $\mathbb{Z}$ no son finitos.

Complemento de un conjunto

El complemento de un conjunto A se define como el conjunto de todos los elementos del conjunto universal que no pertenecen a A. Se

representa por A^c. Por ejemplo, si $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ y $A = \{1, 3, 6, 7, 9\}$, el complemento de A es

$$A^c = \{2, 4, 5, 8\}.$$

Conjunto potencia

Sea A un conjunto. Al conjunto de todos los subconjuntos de A se le llama **conjunto potencia** de A y se representa por $P(A)$ o 2^A.

Por ejemplo, sea $A = \{a, b, c\}$.

El conjunto potencia de A viene dado por

$$P(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \emptyset, A\}$$

El cardinal del conjunto potencia de un conjunto A se define como

$$|P(A)| = 2^{|A|}.$$

Así que el cardinal de $P(A)$, donde A es el conjunto del ejemplo anterior es

$$|P(A)| = 2^{|A|} = 2^3 = 8$$

Una **Familia de conjuntos** es un conjunto cuyos elementos son a su vez conjuntos. Por ejemplo, el conjunto

$$F = \{\{a\}, \{1, 2\}, \{c, b\}, \emptyset, \{4, 5, 6\}\}$$

es una familia de conjuntos. El conjunto

$$G = \{\{b\}, \{3, 4, 5\}, 3, \{c, d\}, 7\}$$

no es una familia de conjuntos. El conjunto potencia de un conjunto A es una familia de conjuntos.

Sea I un conjunto de índices. Una familia de conjuntos también se puede definir como

$$F = \{A_i\}_{i \in I}, \text{ donde los } A_i \text{ son conjuntos.}$$

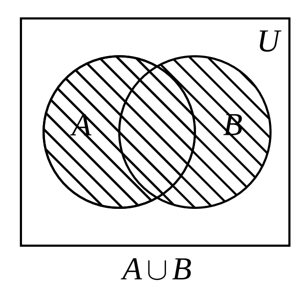
Contenido

Sean A y B dos conjuntos cualesquiera de U.

La **unión** de A y B se define como el conjunto de todos los elementos que pertenecen a A o a B o a ambos. Se representa por $A \cup B$. Simbólicamnete, se escribe

$$A \cup B = \{x \in U | x \in A \text{ o } x \in B\}.$$

El diagrama de Venn para la unión es



$A \cup B$

Ejemplo

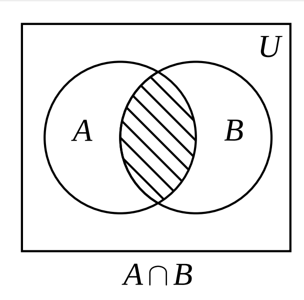
Sean los conjuntos $A = \{a, 5, q\}$ y $B = \{3, a, 7\}$. Entonces

$$A \cup B = \{a, 5, q, 3, 7\}.$$

La **intersección** de A y B se define como el conjunto de todos los elementos comunes a A y a B. Se representa por $A \cap B$. Simbólicamnete, se escribe

$$A \cap B = \{x \in U | x \in A \text{ y } x \in B\}.$$

El diagrama de Venn para la intersección es


U
A
B
$A \cap B$

Ejemplo

Sean los conjuntos $A = \{a, b, 7, d\}$ y $B = \{3, b, c, 7\}$. Entonces

$$A \cap B = \{b, 7\}.$$

Conjuntos disjuntos

Dos conjuntos A y B son **Disjuntos** si no poseen elementos comunes. Es decir, si

$$A \cap B = \emptyset.$$

Ejemplo

Sean $A = \{2, 3, 4, 7\}$ y $B = \{x \in \mathbb{R} | x^2 - 1 = 0\}$. Es claro que $A \cap B = \emptyset$.

Generalización de la unión e intersección

Sea I un conjunto de índices. Suponga que para cada $i \in I$ hay un $A_i \subseteq U$. Entonces generalizando, se tiene

$$\bigcup_{i \in I} A_i = \{x | x \in A_i \text{ para algún } i \in I\}$$

y

$$\bigcap_{i \in I} A_i = \{x | x \in A_i, \ \forall i \in I\}.$$

Si $I = \mathbb{Z}^+$, entonces

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots = \bigcup_{i=1}^{\infty} A_i$$

y

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots = \bigcap_{i=1}^{\infty} A_i$$

Ejemplo

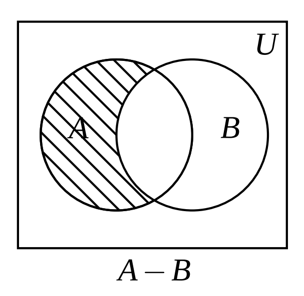
Sean $U = \mathbb{R}$, $I = \mathbb{R}^+$. Suponga que para todo $n \in I$ se tiene que $A_n = [-n, n]$. Entonces

$$\bigcup_{i \in I} A_i = \mathbb{R} \text{ y } \bigcap_{i \in I} A_i = \{0\}$$

La **diferencia** de A menos B se define como el conjunto de todos los elementos que están en A y que no están en B. Se representa por $A - B$. Simbólicamnete, se escribe

$$A - B = \{x \in U | x \in A \text{ y } x \notin B\}.$$

Así que el complemento de A se puede escribir como $A^c = U - A$. El diagrama de Venn para la diferencia es



Ejemplo

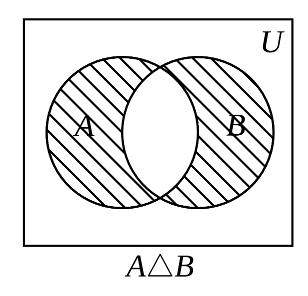
Sean los conjuntos $A = \{4, 5, a, b, 7, d\}$ y $B = \{3, 5, d, e, 7\}$. Entonces

$$A - B = \{4, a, b\}.$$

La **diferencia simétrica** de A y B se define como el conjunto de todos los elementos que están en $A \cup B$ y que no están en $A \cap B$. Se representa por $A \triangle B$. Simbólicamnete, se escribe

$$A \triangle B = \{x \in U | x \in (A \cup B) \text{ y } x \notin (A \cap B)\} = (A \cup B) - (A \cap B).$$

El diagrama de Venn para la diferencia simétrica es



$A \triangle B$

Ejemplo

Sean los conjuntos $A = \{3, 4, a, b, 7, d\}$ y $B = \{2, 4, b, e, 5\}$. Entonces

$$A \triangle B = \{2, 3, a, 7, d, e, 5\}.$$

Contenido

Propiedades de las Operaciones con conjuntos

Conmutativas	**Asociativas**
$A \cup B = B \cup A$ $A \cap B = B \cap A$	$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$
Distributivas	**Idempotencia**
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cup A = A$ $A \cap A = A$

Propiedades de las Operaciones con conjuntos

Complemento	Complemento
$(A^c)^c = A$	$A \cup A^c = U$
$A \cap A^c = \emptyset$	$\emptyset^c = U$
$U^c = \emptyset$	$\emptyset^c = U$

Ley de De Morgan	Ley de De Morgan
$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$
Conjunto universal	**Conjunto universal**
$(A \cup U) = U$	$(A \cap U) = A$
Conjunto vacío	**Conjunto vacío**
$(A \cup \emptyset) = A$	$(A \cap \emptyset) = \emptyset$

Para probar que los conjuntos A y B son iguales ($A = B$), debemos probar que $A \subseteq B$ y $B \subseteq A$.

A modo de ejemplo, probemos una de las leyes de D'Morgan

$$(A \cup B)^c = A^c \cap B^c.$$

Prueba

1. Probemos que $(A \cup B)^c \subseteq A^c \cap B^c$.

Sea $x \in (A \cup B)^c$. Entonces $x \notin (A \cup B)$. De aquí que $x \notin A$ y $x \notin B$. Entonces $x \in A^c$ y $x \in B^c$. Por tanto, $x \in A^c \cap B^c$. Luego, $(A \cup B)^c \subseteq A^c \cap B^c$.

2. Probemos que $A^c \cap B^c \subseteq (A \cup B)^c$.

Sea $x \in A^c \cap B^c$. Entonces $x \in A^c$ y $x \in B^c$. De aquí que $x \notin A$ y $x \notin B$. Entonces $x \notin (A \cup B)$ y por tanto, $x \in (A \cup B)^c$. Luego, $A^c \cap B^c \subseteq (A \cup B)^c$.

Hemos probado que $(A \cup B)^c \subseteq A^c \cap B^c$ y $A^c \cap B^c \subseteq (A \cup B)^c$. Por tanto,

$$(A \cup B)^c = A^c \cap B^c$$

Generalización de las Leyes de D'Morgan

Sea I un conjunto de índices. suponga que para cada $i \in I$ hay un $A_i \subseteq U$. Entonces generalizando, se tiene

$$(\bigcup_{i \in I} A_i)^c = \bigcap_{i \in I} A_i^c$$

y

$$(\bigcap_{i \in I} A_i)^c = \bigcup_{i \in I} A_i^c$$

Teorema

Sean A y B dos conjuntos finitos. Entonces

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

La demostración se bosqueja mediante los diagramas de Venn.

Teorema

Sean A, B, y C conjuntos finitos. Entonces

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|.$$

Ejemplo

Suponga que una Universidad requiere 12 profesores de Matemática y 8 de Física. De estos, 3 deben enseñar ambas materias. ¿Cuántos profesores necesita la Universidad?

Solución

Sea A el conjunto de los profesores de Matemática. Entonces $|A| = 12$ y sea B el conjunto de los profesores de Física.

Entonces $|B| = 8$. Y $|A \cap B| = 3$. Luego, la Universidad necesita $|A \cup B| = |A| + |B| - |A \cap B| = 12 + 8 - 3 = 17$ profesores.

1. Sean los conjuntos:
   $A = \{x | x \in \mathbb{N}, x \text{ par}, \ 0 \ < \ x \ < \ 8\}$
   $B = \{x | x \in \mathbb{Q}, x(x^2 - 6) = 0\}$
   $C = \{x | x \in \mathbb{N}, -x^2 + x + 20 \ > \ 0\}$
   a. Determine por extensión a A, B y C.
   b. Encuentre $P(A)$.
   c. Determine si es verdero o falso y justifique su respuesta
      $4 \subseteq A, \quad 4 \in A, \quad 3 \notin B, \quad -4 \subseteq C, \quad \emptyset \in C, \quad \emptyset \subseteq C,$
      $\{0\} \subseteq C$

2. Sean los conjuntos:
   $A = \{x | x \in \mathbb{N}, -x^2 + 5x \ \geq \ 0\}$
   $B = \{x | x \in \mathbb{N}, 2x + 7 \ < \ 25\}$
   $C = \{x | x \in \mathbb{N}, x^2 \ \geq ; 0\}$
   a. Determine los conjuntos por extensión.
   b. Encuentre
      $A - C, \quad A \cap C, \quad (A - C) \cup (C - A), \quad B \cup A, \quad B \cup A \cup C$

3. ¿Cuáles de los conjuntos siguientes son iguales?
   $E = \{r, t, s\}, \quad F = \{s, t, r, s\}, \quad D = \{t, s, t, r\}, \quad \{s, r, s, t\}$
4. ¿Cuáles de los siguientes conjuntos son finitos?
   a. $\{x | x$ es un dia de las semana$\}$
   b. $\{x | x$ es un número natural impar$\}$
   c. $\{x | x$ es un ser humano de la tierra$\}$

d. $\{1, 2, 3, \ldots, 1000\}$
e. $\{2, 4, 6, \ldots\}$

5. ¿Cuáles de los conjuntos siguientes son iguales?
$\{0\}, \quad \{\emptyset\}, \quad \emptyset$
6. Determine los conjuntos que son vacíos
a. $\{x | x^2 = 9, \; 2x = 4\}$
b. $\{x | x \neq x\}$
c. $\{x | x + 3 = 3\}$
d. $\{x | x^2 \; < \; 0\}$
e. $\left\{ x \,\middle|\, \frac{x+3}{10} = 1/5 \;, \;\; x \in \mathbb{N} \right\}$

7. Demuestre que $A = \{4, 5, 6, 7\}$ no es subconjunto de $B = \{x|x \text{ es par}\}$
8. Demuestre que si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$
9. Encuentre $P(A)$, si $A = \{3, 4, 5\}$
10. Demuestre que si $A \subseteq \emptyset$, entonces $A = \emptyset$.
11. Sean $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}, \quad A = \{1, 2, 3, 4\}, \quad B = \{2, 4, 6, 8\}, \quad C = \{3, 4, 5, 6\}$. Encuentre
    a. $A^c, \quad A \cap C, \quad B - C$
    b. $(A \cap C)^c, \quad A \cup B$

12. En un Hospital de Santo Domingo se tienen los datos siguientes sobre 50 pacientes: 21 sufren de diabetes; 22 sufren del corazón; 10 sufren de diabetes y de la vista; 9 sufren de la vista y el corazón; 6 sufren de diabetes y el corazón; 5 de la vista, diabetes y el corazón. Determine el número de pacientes que:
    a. Sufren de la vista
    b. Sufren sólo de la vista
    c. Sufren de diabetes pero no del corazón
    d. Sufren de la vista pero no de diabetes

13. Demuestre que $(A - B) \cap B = \emptyset$

14. Sean A y B dos conjuntos cualesquiera. Demuestre que $(A \cap B) \subseteq A \subseteq (A \cup B)$

15. En la escuela “Anacleto Pérez” de Anapulla hay una población de estudiantes con las siguientes características: 36 estudian Inglés; 23 estudian Francés; 13 estudian Portugués; 6 estudian Inglés y Francés; 4 estudian Francés y Portugués; 11 estudian Inglés y Portugués; y 1 estudia los tres idiomas. ¿Cuántos estudiantes tiene la escuela?.

16. Sean A, B y C tres conjuntos, de los cuales se conoce:
    a. $C \subseteq (A \cup B)$
    b. $|A \cap B \cap C| = 3$
    c. $|A \cap B| = 3$
    d. $|B \cap C| = 5$
    e. $|A \cap C| = 4$
    f. $|A| = 20$

g. $|A \cup C| = 35$
h. $|A \cup B| = 40$

Hallar el cardinal de los conjuntos B y C.

17. Dibujar un diagrama de Venn de tres conjuntos no vacíos A, B y C tales que satisfagan las propiedades:
    a. $A \subseteq B, \quad C \subseteq B, \quad A \cap C = \emptyset$
    b. $A \subseteq B, \quad C \not\subseteq B, \quad A \cap C \neq \emptyset$
    c. $A \subseteq C, \quad A \neq C, \quad B \cap C = \emptyset$
    d. $A \subseteq (B \cap C), \quad B \subseteq C, \quad C \neq B, \quad A \neq C$
18. Demuestre que si $A \cap B = \emptyset$, entonces $A \subseteq B^c$
19. Demuestre que si $A \subseteq B$, entonces $A \cup (B - A) = B$

20. Sean $U = \{a, b, c, d, e, f, g\}$, $A = \{a, b, c, d, e\}$ $B = \{a, c, e, g\}$, $C = \{b, e, f, g\}$. Encuentre

a. $A \cup C$
b. $B \cap A$
c. $C - B$
d. $B^c \cup C$
e. $C^c \cap A$
f. $(A - C)^c$
g. $(A - B^c)^c$
h. $(A \cap A^c)^c$

Contenido





Definición

El conjunto de los números naturales se define como

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}.$$

El conjunto de los números naturales se puede empezar en cero (0) o en uno (1). Nosotros lo vamos a empezar en cero (0). El conjunto $\mathbb{N}$ es **infinito**.

Definición

Sea A un conjunto no vacío cualquiera. Decimos que una operación $\star$ es **Interna** en A, si para cualesquiera a y b en A se sigue que

$a \star b \in A$. Suele decirse que el conjunto A es **Cerrado** con respecto a la operación $\star$.

Operaciones internas en $\mathbb{N}$: suma (+) y multiplicación (*)

Principio del buen orden

Todo subconjunto no vacío de números naturales tiene un primer elemento o elemento mínimo. Es decir, si $A \subset \mathbb{N}, \quad A \neq \emptyset$, entonces existe $m \in A \quad \ni m \leq n, \, \forall n \in A$.

Teorema

No hay número natural entre 0 y 1.

Demostración

Supongamos que existe un número natural a, tal que $0 < a < 1$. Entonces hay un conjunto $A \neq \emptyset$ de números naturales menores que 1.

Por el principio del buen orden, A tiene un primer elemento, digamos $m \in A$. Entonces $0 < m < 1$. Multiplicando todos los miembros de la última desigualdad por m tenemos que $0 < m^2 < m$. Pero esto contradice el hecho de que m era el elemento mínimo de A.

Por tanto, entre 0 y 1 no hay número natural. ■

Definición

El conjunto de los números enteros se define como

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

El conjunto $\mathbb{Z}$ es **infinito.**

Operaciones internas en $\mathbb{Z}$: suma (+), resta (-) y multiplicación (*).

$$\mathbb{N} \subseteq \mathbb{Z}$$

Contenido

Definición

Sean $a, b \in \mathbb{Z}$. Se dice que a divide a b, escrito $a \mid b$, si existe $k \in \mathbb{Z}$ tal que $b = ka$. Si $a \mid b$ se dice que a es un divisor de b o que b es un múltiplo de a

Ejemplo

$2 \mid 6, \quad 5 \mid 40, \quad 11 \mid 55$

Si a no divide a b, se escribe $a \nmid b$.

Propiedades de la divisibilidad

Sean $a, b, c, d \in \mathbb{Z}$.

a. $1 \mid a, \quad a \mid a, \quad a \mid 0$.

b. Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.
c. Si $a \mid b$, entonces $a \mid bc$ y $ac \mid bc$.
d. Si $a \mid b$ y $a \mid c$, entonces $a \mid b + c$.
e. Si $a \mid b$ y $a \mid c$, entonces $a \mid bx + cy, \quad \forall x, y \in \mathbb{Z}$.
f. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.
g. Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.

División según Euclides

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen enteros únicos q y r, tales que $a = bq + r, \quad 0 \leq r < |b|$.

a es llamado **dividendo**.
b es llamado **divisor**.
q es llamado **cociente**.
r es llamado **resto**.

Definición

Un **factor o divisor** es cada uno de los operandos de un producto.

Ejemplos

La expresión abc tiene como factores a a, b y c.

Los factores de $5x(a+b)$ son : 5, x y $(a+b)$.
Los factores de $(13)(-37)$ son : 13 y -37.

Definición

Un número $p \in \mathbb{N}, \ \ p > 1$ es **primo** si sus únicos divisores en $\mathbb{N}$ son 1 y p. Si un número $n \in \mathbb{N}, \ \ n > 1$ no es primo, decimos que es **compuesto**

Ejemplos

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \ldots$$

El 2 es el único primo par.

Ejemplos

$6, \quad 15, \quad 42, \quad 70$ son compuestos.

Propiedad

Números primos

Si n es un entero compuesto, entonces n tiene al menos un divisor primo menor o igual a $\sqrt{n}$.

El 0 , 1 y los enteros negativos no son primos ni compuestos por definición.

Teorema fundamental de la aritmética

Sea $n \in \mathbb{N}, \;\; n > 1$ no primo. Existen números primos únicos $p_1, p_2, \cdots, p_r$ y enteros no negativos únicos $m_1, m_2, \cdots, m_r$, tales que n se puede expresar de manera única, excepto en el orden de los factores, como

$$n = p_1^{m_1}\, p_2^{m_2}\, \ldots p_r^{m_r}.$$

A esta expresión se le llama **Descomposición factorial** de n en números primos.

Ejemplos

Descomponer los números 18, 70 y 56 en factores primos:

$$18 = 2 * 3 * 3 = 2 * 3^2, \quad 70 = 2 * 5 * 7, \quad 56 = 2 * 2 * 2 * 7 = 2^3 * 7$$

Los factores en los que se descompone el número n se les llama **Divisores** de n.

Definición

Sean $a, b \in \mathbb{Z}$. Decimos que $c \in \mathbb{Z},\ c \neq 0$, es un **Divisor común** de a y b, si $c \mid a$ y $c \mid b$.

Definición

Sean $a, b \in \mathbb{Z}$, con al menos uno de ellos distinto de cero. Se dice que $c \in \mathbb{Z}$ es el **Máximo común divisor** de a y b, denotado por $c = MCD(a, b)$, si y sólo si, se satisfacen las siguientes condiciones:

a. $c \mid a$ y $c \mid b$.
b. c es el mayor divisor común de a y b. Es decir, si d es otro divisor común de a y b, entonces $d \mid c$.
c. $c > 0$

Ejemplo

Calcular el $MCD(24, 18)$.

El conjunto de los divisores de 24 es: $\{1, 2, 3, 4, 6, 8, 12, 24\}$.

El conjunto de los divisores de 18 es: $\{1, 2, 3, 6, 9, 18\}$.

El conjunto de los divisores comunes es: $\{1, 2, 3, 6\}$.

El mayor de los comunes es el 6. Así que el

$$MCD(24, 18) = 6.$$

Propiedades

Sean $a, b \in \mathbb{Z}$, con al menos uno de ellos distinto de cero. Entonces

a. $MCD(a, b) \geq 0$

b. $MCD(a, b) = MCD(b, a)$

c. $MCD(0, a) = |a|$

d. $MCD(ka, a) = |a|, \quad \forall k \in \mathbb{N}$

e. $MCD(-a, b) = MCD(a, -b) = MCD(-a, -b) = MCD(a, b) = MCD(|a|, |b|)$

f. Si $a = b = 0$, entonces para todo $c \in \mathbb{Z}$, c es un divisor común de a y b. Por tanto, no existe un $MCD(a, b)$.

g. El $MCD(a, b)$ es único.

h. $MCD(ka, kb) = |k| \, MCD(a, b), \ \forall k \neq 0$

Procedimiento para calcular el $MCD(a,b)$

Sean $a,b \in \mathbb{N}, \;\; a,b > 1$.

Se descompone a y b en sus factores primos. Luego, el producto de los factores comunes elevados al menor exponente es el $MCD(a,b)$. Es decir, suponga que

$$a = \pm p_1^{k_1}\, p_2^{k_2}\, p_3^{k_3} \ldots p_r^{k_r}$$

y

$$b = \pm p_1^{l_1}\, p_2^{l_2}\, p_3^{l_3} \ldots p_r^{l_r},$$

donde $k_i, l_i \geq 0$.

Entonces

$$MCD(a,b) = p_1^{\min\{k_1,l_1\}}\, p_2^{\min\{k_2,l_2\}}\, p_3^{\min\{k_3,l_3\}} \ldots p_r^{\min\{k_r,l_r\}}$$

Ejemplo

Calcular $MCD(2520, 4950)$.

$$\begin{aligned} 2520 &= 2^3 \,.\, 3^2 \,.\, 5 \,.\, 7 \\ 4950 &= 2 \,.\, 3^2 \,.\, 5^2 \,.\, 11 \end{aligned}$$

Luego, el

$$MCD(2520, 4950) = 2^1 \,.\, 3^2 \,.\, 5^1 = 90.$$

Teorema

Sean $a, b, q, r \in \mathbb{N}$, con $a = bq + r, \quad 0 \leq r < b$. Entonces

$$MCD(a, b) = MCD(b, r).$$

Ejemplo

$24 = 18 * 1 + 6(a = 24,\ b = 18,\ q = 1,\ r = 6)$

$18 = 6 * 3 + 0$

Luego,

$$MCD(24, 18) = MCD(18, 6) = 6.$$

Definición

Sean $a, b \in \mathbb{Z}$. Decimos que a y b son **Primos relativos o coprimos o primos entre si**, si los únicos divisores comunes de a y b son 1 y -1. Es decir, $MCD(a, b) = 1$.

Ejemplo

El 8 y el 35 son primos relativos.

Teorema

Sean $a, b \in \mathbb{Z}$ con al menos uno de ellos distinto de cero. Entonces a y b son primos entre si, si y sólo si, existen $x_0, y_0 \in \mathbb{Z}$, tales que

$$ax_0 + by_0 = 1.$$

Contenido

Algoritmo de Euclides

Sean $a, b \in \mathbb{N},\ \ a \geq b > 0$. Sea $r_0 = a,\ \ r_1 = b$. Aplicando en forma sucesiva la división según Euclides, se tiene

$$\begin{array}{rcl} r_0 & = & r_1 q_1 + r_2, \quad 0 < r_2 < r_1 \\ r_1 & = & r_2 q_2 + r_3, \quad 0 < r_3 < r_2 \\ & & \ldots \qquad \ldots \qquad \ldots \\ r_k & = & r_{k+1} q_{k+1} + r_{k+2}, \quad 0 < r_{k+2} < r_{k+1} \\ & & \ldots \qquad \ldots \qquad \ldots \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_n q_n + r_{n+1}, \quad r_{n+1} = 0 \end{array}$$

Luego, el $MCD(a, b) = r_n$, donde r_n es el último resto no nulo.

Nota: La sucesión $\{r_n\}_{n\geq 1}$ es finita, puesto que

$$r_1 > r_2 > r_3 > \cdots \geq 0. \text{ (estríctamente decreciente)}$$

Ejemplo

Calcular $MCD(24, 18)$.

Solución

En este caso $r_0 = a = 24$, $r_1 = b = 18$. Si se divide 24 entre 18, se obtiene $r_0 = r_1 * q_1 + r_2, \;\; 0 < r_2 < r_1$. Es decir, $24 = 18 * 1 + 6, \;\; 0 < 6 < 18$. Como $r_2 \neq 0$, se divide $r_1 = 18$ entre

$r_2 = 6$ y se obtiene $r_1 = r_2 q_2 + r_3$, donde $r_3 = 0$. Como r_2 es el último residuo distinto de cero, tenemos que

$$MCD(24, 18) = r_2 = 6.$$

Ejemplo

Calcular $MCD(25134, 19185)$.

Solución

En este caso $r_0 = 25134, \;\; r_1 = 19185$

$$\begin{aligned}
r_0 &= r_1 * q_1 + r_2 = 19185 * 1 + 5949\\
r_1 &= r_2 * q_2 + r_3 = 5949 * 3 + 1338\\
r_2 &= r_3 * q_3 + r_4 = 1338 * 4 + 597\\
r_3 &= r_4 * q_4 + r_5 = 597 * 2 + 144\\
r_4 &= r_5 * q_5 + r_6 = 144 * 4 + 21\\
r_5 &= r_6 * q_6 + r_7 = 21 * 6 + 18\\
r_6 &= r_7 * q_7 + r_8 = 18 * 1 + 3\\
r_7 &= r_8 * q_8 + r_9 = 3 * 6 + 0.
\end{aligned}$$

Luego,

$$MCD(25134, 19185) = r_8 = 3 \text{ último resto distinto de cero.}$$

1. Sean $a, c \in \mathbb{Z}$ y $b \in \mathbb{N}$. Suponga que $2b$ está a la derecha de a; que a su vez, está a la derecha de b. Suponga que c está a la izquierda de 0. ¿Cual de la siguientes afirmaciones es falsa?:

   a. $2b > b$ b. $c < 0$ c. $a > b$ d. $b > 0$ e. $a < c$

2. Si a y b son enteros consecutivos y $a < b$, entonces cuál de las siguientes afirmaciones es verdadera para $b - a$?

   a. 0 b. -1 c. $3a + 2$ d. 1 e. $a - b$

3. Si $a, b \in \mathbb{Z}$ y b es el predecesor de a, y el sucesor de a es -9 , entonces cuál de las siguientes afirmaciones es verdadera para $a + b$?

   a. -15 b. -17 c. -21 d. -20 e. -19

4. Si a es un entero par y b es un entero impar, entonces ¿cuál de las siguientes afirmaciones es (son) siempre verdadera(s)?

   a. Sólo a^2 es un número positivo
   b. Sólo $-b^2$ es un número positivo
   c. Sólo $(a - b)^2$ es un número impar positivo
   d. Sólo a. y c.
   e. Sólo b. y c.
   f. Ninguna de las anteriores

5. Aplique el algoritmo de Euclides para encontrar $MCD(1001, 275), \quad MCD(687, -234)$.
6. Sea $m \in \mathbb{Z}^+$. Pruebe que $(k+1)(k+2)(k+3)\cdots(k+m), \quad k \geq 0$ es divisible por $m!$.
7. Sea $n \in \mathbb{Z}^+$. Pruebe que $(n!)^2$ divide a $(2n)!$.
8. Sean $a, b, c, d \in \mathbb{Z}^+$, pruebe que si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$

9 Pruebe que el producto de tres (3) enteros consecutivos es divisible por 6. Además, 24 divide al producto si el primero es par.

10. Pruebe que $100 \mid (11^{10} - 1)$
11. Sea $n \in \mathbb{Z}^+$. Pruebe que $30 \mid (n^5 - n)$
12. Pruebe que si $n = st, \quad s > 0, t > 0$, entonces $(s!)^t \mid n!$

13. Sean $n, m \in \mathbb{Z}^+$ y $a > 1$. Pruebe que $(a^n - 1) \mid (a^m - 1)$, si y sólo si $n \mid m$
14. Encuentre aplicando el algoritmo de Euclides:
    a. $MCD(72, 16)$
    b. $MCD(80, 32)$
    c. $MCD(848, 656)$
    d. $MCD(93164, 5826)$
    e. $MCD(279492, 17478)$
    f. $MCD(3907853, 3802499)$
15. Pruebe que $MCD(a, b)$ es único.

Definición

Sean $a, b \in \mathbb{Z} - \{0\}$. El **Mínimo común múltiplo** de a y b, representado por $MCM(a, b)$, es el único entero positivo c que satisface las condiciones siguientes:

1. $a \,|\, c$ y $b \,|\, c$ (esto dice que c es múltiplo común).
2. Si $a \,|\, d$ y $b \,|\, d$ con $d > 0$, entonces $c \leq d$ (significa esto que c es el menor de los múltiplos positivos comunes de a y b).

Mínimo común múltiplo

Definición

Sean $a, b \in \mathbb{Z} - \{0\}$. El $MCM(a, b)$ se define como

$$MCM(a, b) = \frac{|ab|}{MCD(a, b)}.$$

Procedimiento para calcular el $MCM(a, b)$

1. Se descompone a y b en sus factores primos.
2. El $MCM(a, b)$ es el producto de los factores comunes y no comunes, con los factores comunes elevados a su mayor exponente.

Suponga que

$$a = \pm p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_r^{k_r}$$

y

$$b = \pm p_1^{l_1} p_2^{l_2} p_3^{l_3} \dots p_r^{l_r},$$

donde $k_i, l_i \geq 0$.

Entonces

$$MCM(a,b) = p_1^{\text{máx}\{k_1,l_1\}} p_2^{\text{máx}\{k_2,l_2\}} p_3^{\text{máx}\{k_3,l_3\}} \dots p_r^{\text{máx}\{k_r,l_r\}}$$

Ejemplo

Calcular el $MCM(72, 16)$.

Solución

$72 = 2^3 \times 3^2$

$16 = 2^4$

Luego,

$$MCM(72, 16) = 2^4 \times 3^2 = 16 \times 9 = 144.$$

Observe que se obtiene el mismo resultado si utilizamos la fórmula dada en la definición.

Ejemplo

Calcular $MCM(2520, 4950)$.

$$\begin{aligned} 2520 &= 2^3 \,.\, 3^2 \,.\, 5 \,.\, 7 \\ 4950 &= 2 \,.\, 3^2 \,.\, 5^2 \,.\, 11 \end{aligned}$$

Luego, el

$$MCM(2520, 4950) = 2^3 \,.\, 3^2 \,.\, 5^2 \,.\, 7^1 \,.\, 11^1 = 138600.$$

1. Encuentre el Mínimo común múltiplo de :
   a. 15 y 18
   b. 721 y 448
   c. 424 y 328
2. Pruebe que $MCM(a, b)$ es único.

Contenido



Función característica

Definición

Por el momento, asumamos que una **función** es una regla que asigna un único valor a cada elemento de un conjunto.

Sea A un subconjunto del conjunto universal U. La **función característica** f_A del conjunto A se define como:

$$f_A(x) = \begin{cases} 1, & \text{si } x \in A \\ 0, & \text{si } x \notin A \end{cases}$$

Como la función característica es numérica, puede ser operada aritméticamente.

Propiedades de las funciones características

Teorema

1. $f_{A\cap B}(x) = f_A(x)\, f_B(x), \ \ \forall x$
2. $f_{A\cup B}(x) = f_A(x) \,+\, f_B(x) - f_A(x)\, f_B(x), \ \ \forall x$
3. $f_{A\triangle B}(x) = f_A(x) \,+\, f_B(x) - 2\, f_A(x)\, f_B(x), \ \ \forall x$

Demostración

Parte 1.

$f_A(x)\, f_B(x) = 1 \Longleftrightarrow f_A(x) = 1$ y $f_B(x) = 1$. Esto sólo ocurre, si $x \in A$ y $x \in B$. Es decir, si $x \in (A \cap B)$.
Como $f_A(x)\, f_B(x) = 1$ en $A \cap B$ y 0 fuera de $A \cap B$, se tiene que $f_{A\cap B}(x) = f_A(x)\, f_B(x)$

Parte 2.

Función característica

Si $x \in A$, se tiene que $x \in (A \cup B)$ y $f_A(x) = 1$. Luego,

$$f_{A\cup B}(x) = f_A(x) + f_B(x) - f_A(x)\, f_B(x) = 1 + f_B(x) - f_B(x) = 1.$$

Del mismo modo, si $x \in B$, se tiene que $x \in (A \cup B)$ y $f_B(x) = 1$. Luego,

$$f_{A\cup B}(x) = f_A(x) + f_B(x) - f_A(x)\, f_B(x) = f_A(x) + 1 - f_A(x) = 1.$$

Si $x \notin A$ y $x \notin B$.

Es decir, si $x \notin (A \cup B)$, entonces $f_A(x) = 0$ y $f_B(x) = 0$, por lo que $f_A(x) + f_B(x) - f_A(x)\, f_B(x) = 0$.

De modo que $f_A(x) + f_B(x) - f_A(x)\, f_B(x) = 1$ en $A \cup B$ y 0 fuera de $A \cup B$, por lo que es igual a $f_{A\cup B}(x)$.

Parte 3.

Si $x \in A \triangle B$, se tiene que $x \in (A \cup B)$ y $x \notin (A \cap B)$. Esto quiere decir que $x \in A$ o $x \in B$, pero no de ambos al mismo tiempo.

Si $x \in A$ entonces $x \notin B$, por lo que $f_A(x) = 1, \; f_B(x) = 0$ y $f_A(x) + f_B(x) - 2f_A(x)\, f_B(x) = 1 + 0 - 2(0) = 1$

Si $x \in B$ entonces $x \notin A$, por lo que $f_A(x) = 0, \; f_B(x) = 1$ y $f_A(x) + f_B(x) - 2f_A(x)\, f_B(x) = 0 + 1 - 2(0) = 1$

Luego, $f_A(x) + f_B(x) - 2f_A(x)\, f_B(x) = 1$ para $x \in (A \triangle B)$ y 0 fuera de $(A \triangle B)$, por lo que es igual a $f_{A \triangle B}(x)$.

Contenido



En los conjuntos el orden en que están colocados los elementos (se entiende que son diferentes) no tiene importancia.

Sucesión

Una **sucesión** es una lista de objetos, colocados uno después del otro y numerados según el orden de $\mathbb{Z}^+$. Si la sucesión se detiene después de un número finito de términos, se dice que es **finita**. En caso contrario, se dice que es **infinita**. Los términos de una sucesión son siempre elementos de un conjunto.
Por ejemplo, la lista

$$1,\ 3,\ 5,\ 7, \ldots, (2n-1), \ldots,$$

donde $n \in \mathbb{Z}^+$, es una sucesión infinita.

El conjunto correspondiente a la sucesión es

$$\{1,\ 3,\ 5,\ 7, \dots\}$$

Sea s una sucesión. EL número de objetos que forman la sucesión s se le llama **longitud de** s y se representa por $|s|$. Por ejemplo, la sucesión $s = 2, 4, 6, 8, 10$ es de longitud $|s| = 5$.
En una sucesión los elementos no tienen que ser diferentes. Por ejemplo, la sucesión

$$1,\ 1,\ 1,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1$$

es finita y además tiene elementos repetidos.

El conjunto correspondiente a esta sucesión es

$$\{0,\ 1\}.$$

En general, las sucesiones se escriben como $x_1, x_2, x_3, \ldots$ o como $(x_i)_{i=1}^{\infty}$. Observe que los x_i no tienen que ser números. Cuando la sucesión es finita se puede escribir como $(x_i)_{i=1}^{n}$, donde n es el número de términos.
Por ejemplo, la palabra `bcbbccbbbccc` puede ser interpretada como una sucesión finita o como la lista `b, c, b, b, c, c, b, b, b, c, c, c`, cuyo conjunto es {`b, c`}.

Si se escribe la palabra `abcabcabc...` o `a, b, c, a, b, c, a, b, c,...` decimos que se tiene una sucesión infinita. Su conjunto correspondiente es {`a, b, c`}

En términos computacionales, a las sucesiones se les llama en ocasiones **arreglo lineal**. Un arreglo en computación es una lista de posiciones que siguen el orden del conjunto $\mathbb{Z}^+$.

Como a los términos de una sucesión le corresponde un orden, se puede establecer una correspondencia entre los términos de la sucesión y las posiciones del arreglo. De modo tal que el primer término de la sucesión le corresponda la primera posición del arreglo; al segundo término, la segunda posición del arreglo y así sucesivamente.

Si X es un arreglo, sus posiciones las representamos como $X(1), X(2), X(3), \ldots$ o como $X[1], X[2], X[3], \ldots$.

Si consideramos la sucesión $X = x_1, x_2, x_3, \ldots$, podemos hacer que sus términos ocupen respectivamente las posiciones del arreglo X. De modo que los elementos del conjunto correspondiente a una sucesión X se pueden asignar a las posiciones del arreglo X. Así el término x_n ocupará la posición n del arreglo X, representada por $X(n)$.
Un conjunto A es **numerable o contable** si es el conjunto correspondiente a una sucesión. Es decir, si sus elementos se pueden arreglar en una lista donde haya un primer elemento, segundo, tercero,....

Los conjuntos cuyos elementos no se pueden contar se les llama **no numerables o no contables**.

Se puede probar que todo conjunto finito es numerable.

EL conjunto de números reales en el intervalo $(0, 1)$ es no numerable.

Contenido

Se sabe que el orden de los elemntos en un conjunto carece de importancia, sin embargo, para representarlo en una computadora debemos suponer que sus elementos coresponden a una sucesión. Es decir, que hay un primer, un segundo, un tercer elemento, etc. Sea $U = \{x_1, x_2, \ldots, x_n\}$ un conjunto universal finito. Sea A un subconjunto de U. Entonces podemos definir la función característica de A como:

$$f_A(x) = \begin{cases} 1, & \text{si } \; x \in A \\ 0, & \text{si } \; x \notin A \end{cases}$$

De modo que todo subconjunto se puede representar como una sucesión de longitud n, de ceros y unos.

Ejemplo

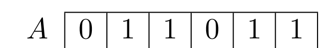
Sean $U = \{a, b, c, d, e, f\}$, $A = \{a, b\}$, $B = \{b, d, f\}$. Entonces $f_A(x)$ está representada por la sucesión $1, 1, 0, 0, 0, 0$. De la misma manera, la sucesión $0, 1, 0, 1, 0, 1$ representa a $f_B(x)$.

De manera que todo conjunto universal U, de cardinal finito n , puede representarse en una computadora como un arreglo X, de tamaño n. Cualquier subconjunto de U se puede representar en la computadora asignando a cada posición de memoria $X(n)$ un uno o un cero, dependiendo de que el elemento pertenezca o no al subconjunto.

Ejemplo

Sea $U = \{a, b, c, d, e, f\}$, $A = \{b, c, e, f\}$. Entonces

U	1	1	1	1	1	1



O sea que

$$A(i) = \begin{cases} 1, & \text{para } i = 2, 3, 5, 6 \\ 0, & \text{para } i = 1, 4 \end{cases}$$

es el arreglo que representa al subconjunto A.

Contenido

Álgebras booleanas

La unidad de información más pequeña dentro de un computador digital es el **bit** ("0" ó "1"). De aquí que exista una relación directa entre la lógica, que utiliza como característica fundamental el valor de verdad de las proposiciones ("verdadera (V)" o "Falsa (F)") y una álgebra booleana que tiene como elementos básicos dos valores, generalmente representados por "0" o "1".

Las tablas lógicas correspondientes al **Not($\neg$)**, **AND ($\wedge$)** y **OR ($\vee$)** en un álgebra booleana son:

p	$\neg p$
1	0
0	1

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Definición

Un **álgebra booleana** B, es un conjunto S, junto con dos operaciones binarias y una operación unaria, generalmente representadas por $+$, $*$ y $'$, y que satisface las siguientes propiedades: Para todo $x, y, z \in S$

a. Propiedades asociativas

$$\begin{aligned}(x+y)+z &= x+(y+z)\\ (x*y)*z &= x*(y*z)\end{aligned}$$

b. Propiedades conmutativas

$$x+y=y+x, \qquad x*y=y*x$$

c. Propiedades distributivas

$$\begin{aligned}x*(y+z) &= (x*y)+(x*z)\\ x+(y*z) &= (x+y)*(x+z)\end{aligned}$$

d. Propiedades de identidad (Elementos neutros)

$$\exists\, 0,\ 1 \in S,\ 0 \neq 1,\ \ni\ x + 0 = x, \qquad x * 1 = x$$

e. Propiedades de complementos

$$x + x' = 1 \qquad x * x' = 0$$

Se escribe $B = (S, +, *, ')$

Ejemplo

Sea $S = \{0, 1\}$. Se puede comprobar que $B = (S, +, *, ')$ es una álgebra booleana, donde las operaciones se definen como

$+$	0	1
0	0	1
1	1	1

$*$	0	1
0	0	0
1	0	1

x	x'
0	1
1	0

Ejemplo

Sea U un conjunto no vacío y $S = P(U)$ el conjunto potencia de U, con la unión, intersección y complemento de conjuntos como operaciones internas en S. Se puede comprobar que $B = (S, \cup, \cap, ')$ es una álgebra booleana.

Aquí $\cup$ hace las veces de la operación $+$, $\cap$ sustituye la operación $*$, y los conjuntos $\emptyset$ y U (conjunto universal) representan los elementos 0 y 1, respectivamente.

Ejemplo

Sea S el conjunto de proposiciones representadas por las variables proposicionales $\{p, q, r, \ldots\}$, junto con las conectivas lógicas Disyunción, Conjunción y Negación del cálculo proposicional. Se puede comprobar que $B = (S, \vee, \wedge, \neg)$ es una álgebra booleana.

Aquí $\vee$ hace las veces de la operación $+$, $\wedge$ sustituye la operación $*$, y $\neg$ toma el lugar de $'$. Los valores de verdad F y V representan los elementos 0 y 1, respectivamente.

Definición

La fórmula **dual** de una fórmula F correspondiente a un álgebra booleana se obtiene de F intercambiando entre si las operaciones suma $(+)$ y multiplicación $(*)$ y los elementos neutros 0 y 1.

Principio de dualidad (teorema)

Si la fórmula F se deriva de los axiomas del álgebra de boole, entonces la dual de F también se deriva de los axiomas del álgebra de boole.

Demostración

Si la fórmula F se deriva aplicando una sucesión de los axiomas del álgebra de boole, la fórmula dual de F se obtiene mediante la

aplicación de una sucesión de los duales de los axiomas del álgebra de boole. ■

Con fines de simplificar la notación, la disyunción debe interpretarse como una suma booleana y la conjunción como un producto booleano. De la misma manera cuando haya posibilidad de confusión en la notación, utilizaré el símbolo $\oplus$ para la suma booleana y $\odot$ para el producto booleano. Para el producto elemento a elemento, usaré el símbolo $\cdot$.

Contenido

Definición

Un objeto matemático de la forma (a, b) se le llama **Par o Pareja ordenada**. a recibe el nombre de **Primera componente** del par ordenado y b recibe el nombre de **Segunda componente** del par ordenado.

Es claro que $(a, b) \neq (b, a)$.

Definición

Sean A y B dos conjuntos. EL **Producto cartesiano o conjunto producto** de A y B se define como

$$A \times B = \{(a, b)|a \in A, b \in B\}.$$

Es claro que $A \times B \neq B \times A$.

Si A y B son finitos, se tiene que $|A \times B| = |A||B|$. Si alguno de los conjuntos A o B es vacío, el conjunto $A \times B$ es vacío.

Ejemplo

Sean $A = \{3, 4, 5\}$ y $B = \{a, b\}$

$A \times B = \{(3, a), (3, b), (4, a), (4, b), (5, a), (5, b)\}$

$B \times A = \{(a, 3), (a, 4), (a, 5), (b, 3), (b, 4), (b, 5)\}$

De forma similar, si alguno de los conjuntos A o B es infinito y el otro no es vacío, el producto cartesiano $A \times B$ es infinito.

Generalizando a n conjuntos $A_1, A_2, A_3, \ldots, A_n$, se tiene que

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) | a_i \in A_i, \;\; i = 1, 2, \ldots, n\}.$$

Ejemplo

Sean $A = \{3, 4, 5\}$, $B = \{a, b\}$ y $C = \{r, s\}$

Producto cartesiano o conjunto producto

$$\begin{aligned} A \times B \times C &= \{(3,a,r),(3,a,s),(3,b,r),(3,b,s),\\ &(4,a,r),(4,a,s),(4,b,r),(4,b,s),\\ &(5,a,r),(5,a,s),(5,b,r),(5,b,s)\} \end{aligned}$$

Definición

El **Conjunto de verdad** de una proposición p es el conjunto de n-uplas de los valores de verdad de las proposiciones simples que la forman que la hacen verdadera. Se representa por $T(p)$. Por ejemplo, consideremos la proposición

$$(p \to q) \wedge (\neg r \veebar q).$$

Su tabla de verdad es

p	q	r	$\neg r$	$(p \to q)$	$(\neg r \veebar q)$	$(p \to q) \wedge (\neg r \veebar q)$
V	V	V	F	V	V	V
V	V	F	V	V	F	F
V	F	V	F	F	F	F
V	F	F	V	F	V	F
F	V	V	F	V	V	V
F	V	F	V	V	F	F
F	F	V	F	V	F	F
F	F	F	V	V	V	V

En este ejemplo

$$\begin{aligned} U &= \{(V,V,V),(V,V,F),(V,F,V),(V,F,F),\\ &\quad (F,V,V),(F,V,F),(F,F,V),(F,F,F)\} \end{aligned}$$

y el conjunto de verdad es

$$T(p) = \{(V,V,V),(F,V,V),(F,F,F)\}.$$

Existe una estrecha relación entre las operaciones entre conjuntos y los operadores lógicos.

Teorema

Sean p y q proposiciones. Entonces

a. $T(p \wedge q) = T(p) \cap T(q)$

b. $T(p \vee q) = T(p) \cup T(q)$

c. $T(\neg p) = (T(p))^c$

d. $p \Longrightarrow q$ si y sólo si $T(p) \subseteq T(q)$

Ejercicios

1. Sean $D = \{\text{Luis, Pedro, Juan}\}$ y $E = \{\text{María, Fifa}\}$. Encuentre $D \times E$ y $E \times D$.
2. Si $(x + y, 1) = (3, x - y)$, encuentre x y y.
3. Sean $A = \{a, b, c\}$, $B = \{2, 4\}$ y $C = \{3, 4, 5\}$. Encuentre $A \times B \times C$
4. Sean $A = \{a, b\}$, $B = \{2, 3\}$ y $C = \{3, 4\}$. Encuentre
   a. $A \times (B \cup C)$
   b. $(A \times B) \cup (A \times C)$
   c. $A \times (B \cap C)$
   d. $A \times B) \cap (A \times C)$
5. Demuestre que $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Ejercicios

6. Sean $A \subseteq B$ y $C \subseteq D$. Demuestre que $(A \times C) \subseteq (B \times D)$.
7. Encuentre el conjunto de verdad de $p \wedge \neg q$.
8. Encuentre el conjunto de verdad de $\neg p \to q$.
9. Encuentre el conjunto de verdad de $(p \vee q) \wedge r$.
10. Suponga que la proposición $P = P(p, q, r, \dots)$ es una tautología. Encuentre el conjunto de verdad $T(P)$.
11. Suponga que la proposición $P = P(p, q, r, \dots)$ es una contradicción. Encuentre el conjunto de verdad $T(P)$.
12. Sean $P = P(p, q, r, \dots)$ y $Q = Q(p, q, r, \dots)$ proposiciones tales que $P \wedge Q$ es una contradicción. Demuestre que los conjuntos $T(P)$ y $T(Q)$ son disjuntos.

13. Demuestre que $A \times (B \cup C) = (A \times B) \cup (A \times C)$
14. Si $(y - 2, 2x + 1) = (x - 1, y + 2)$. Encuentre x y y.
15. Encuentre el conjunto de verdad de $p \leftrightarrow \neg q$
16. Encuentre el conjunto de verdad de $\neg p \vee \neg q$
17. Encuentre el conjunto de verdad de $(p \rightarrow q) \wedge (p \leftrightarrow r)$
18. Sea $A = B \cap C$. Determine cuál de las expresiones siguientes es verdadera.
    - a $A \times A = (B \times B) \cap (C \times C)$
    - b $A \times A = (B \times C) \cap (C \times B)$

Contenido

Inducción matemática

Sea $P(n)$ una función proposicional cuyo dominio de referencia es $\mathbb{N}$. Sea $n_0 \in \mathbb{N}$ fijo. Se desea demostrar que $P(n)$ es verdadera para toda $n \geq n_0$. Suponga que:

a. $P(n_0)$ es verdadera. (**paso base o básico**).

b. $\forall n \geq n_0 : [P(n) \Rightarrow P(n+1)]$ (**paso inductivo**).

Entonces el **Principio de inducción matemática** establece que $P(n)$ es verdadera para toda $n \geq n_0$.

Ejemplo

Demostrar por inducción matemática que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}, \quad n \geq 1.$$

Demostración

Aquí $P(n)$ es la función proposicional

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \text{ y } n_0 = 1.$$

a. **paso básico:** comprobar que $P(n)$ es verdadera para $n = 1$.

$$1 = \frac{1(1+1)}{2}$$

b. **paso inductivo:** Suponer que $P(n)$ es verdadera, para probar que $P(n+1)$ es verdadera. Es decir, suponer que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

es cierta para algún $n \geq 1$. Ahora probaré que $P(n+1)$ es verdadera.

Consideremos la expresión

$$\sum_{i=1}^{n+1} i = 1+2+3+\cdots+n+(n+1) = \frac{n(n+1)}{2} + (n+1)$$
$$= \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Esto prueba que $P(n+1)$ es verdadera. Por tanto, $P(n)$ es verdadera para toda $n \geq 1$.

Ejemplo

Sean $A_1, A_2, A_3, \ldots, A_n$ subconjuntos de un conjunto universal U. Demostrar por inducción matemática que

$$\left(\bigcup_{i=1}^{n} A_i\right)^c = \bigcap_{i=1}^{n} A_i^c, \quad n \geq 1$$

Demostración

Aquí la función proposicional $P(n)$ es la igualdad anterior.

a. **Paso básico:** comprobar que $P(n)$ es verdadera para $n = 1$.

$$A_1^c = A_1^c$$

b. **Paso inductivo:** suponer que $P(n)$ es verdadera, para probar que $P(n+1)$ es verdadera. Es decir suponer que

$$\left(\bigcup_{i=1}^{n} A_i\right)^c = \bigcap_{i=1}^{n} A_i^c, \quad n \geq 1$$

es verdadera. Sean $A_1, A_2, A_3, \ldots, A_n, A_{n+1}$ subconjuntos de U y sea $B = A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$. Entonces

$$\begin{aligned}
\left(\bigcup_{i=1}^{n+1} A_i\right)^c &= (B \cup A_{n+1})^c = B^c \cap A_{n+1}^c = \left(\bigcup_{i=1}^{n} A_i\right)^c \cap A_{n+1}^c \\
&= \left(\bigcap_{i=1}^{n} A_i^c\right) \cap A_{n+1}^c = \bigcap_{i=1}^{n+1} A_i^c.
\end{aligned}$$

Luego, $P(n+1)$ es verdadera. Por tanto, $P(n)$ es verdadera para toda $n \geq 1$.

Definición

Sea $n \in \mathbb{Z}, \ \ n \geq 0$. Entonces n factorial se define como

$$n! = \begin{cases} 1, & n = 0 \\ n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1, & n > 0 \end{cases}$$

Ejemplos

$$3! = 3 \cdot 2 \cdot 1 = 6, \quad 5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120, \quad 1! = 1, \quad 2! = 2 \cdot 1 = 2$$

Note que $n! = n(n-1)!$.

Ejemplo

Demostrar por inducción matemática que

$$n! \geq 2^{n-1}, \ \forall n \geq 1.$$

Demostración

a. **Paso base:** Comprobar que $P(n)$ es verdadera para $n = 1$.

$$1! \geq 2^0.$$

b. **Paso inductivo:** suponer que $P(n)$ es verdadera, para probar que $P(n+1)$ es verdadera. Es decir suponer que

$$n! \geq 2^{n-1}$$

es verdadera.

Debemos probar que

$$(n+1)! \geq 2^n.$$

Observemos que

$$(n+1)! = (n+1)n! \geq (n+1)2^{n-1} \geq 2 \,.\, 2^{n-1} = 2^n.$$

Luego, $P(n+1)$ es verdadera. Por tanto, $P(n)$ es verdadera para toda $n \geq 1$.

Ejemplo

Demostrar por inducción matemática que

$$7^n - 1$$

es divisible por 6 para toda $n \geq 1$.

Demostración

a. **Paso base:** comprobar que $P(n)$ es verdadera para $n = 1$.

$$7^1 - 1 = 6$$

es divisible entre 6.

b. **Paso inductivo:** Suponer que $P(n)$ es verdadera, para probar que $P(n+1)$ es verdadera. Es decir, debemos asumir que

$$7^n - 1, \quad \text{es divisible entre 6.}$$

Ahora, tomemos la expresión

$$7^{n+1} - 1 = 7\,.\,7^n - 1 = 6\,.\,7^n + 1\,.\,7^n - 1.$$

Como $6\,.\,7^n$ y $1\,.\,7^n - 1$ (hipótesis inductiva) son divisibles entre 6, su suma también lo es. Luego, $P(n+1)$ es verdadera. Por tanto, $P(n)$ es verdadera para toda $n \geq 1$.

Inducción matemática fuerte

Sea $P(n)$ una función proposicional, cuyo dominio de referencia es el conjunto $D = \{n \in \mathbb{Z} \,|\, n \geq n_0\}$. Suponga que

a. $P(n_0)$ es verdadera.

b. $\forall n > n_0,$ si $P(k)$ es verdadera $\forall k, \ni n_0 \leq k < n$ entonces $P(n)$ es verdadera.

Entonces $P(n)$ es verdadera para todo entero $n \geq n_0$.

1. Pruebe por inducción matemática.
   a. $2n + 1 < 2^n, \quad n \geq 3$
   b. $\sum_{i=1}^{n} i(i+2) = n(n+1)(2n+7)/6$
   c. $\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$
   d. $\sum_{i=1}^{n} 2i = n(n+1)$
   e. $\sum_{i=1}^{n} (2i-1)^2 = \frac{n(2n+1)(2n-1)}{3}$

f. $\sum_{i=1}^{n}(3i-1) = \frac{n(3n+1)}{2}$

g. $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$

2. Considere la sucesión de Fibonacci $F_i = F_{i-1} + F_{i-2},\ i = 3, 4, \ldots,\ F_1 = 1,\ F_2 = 1$. Pruebe por inducción

   a. $\sum_{i=1}^{n-2} F_i = F_n - 1, \ \forall\, n \geq 3.$

   b. $F_n < (5/3)^n, \ \forall\, n \geq 1.$

   c. $F_n < [(1+\sqrt{5})/2]^n, \ \forall\, n \geq 1.$

3. Pruebe por inducción matemática.

a. $\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

b. $\sum_{i=1}^{n} (2i-1) = 1 + 3 + 5 + \cdots + (2n-1) = n^2$

c. $\sum_{i=1}^{n} (-1)^{i+1} i^2 = 1^2 - 2^2 + 3^2 - \cdots + (-1)^{n+1} n^2 = \frac{(-1)^{n+1} n(n+1)}{2}$

d. $\sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)} = \frac{1}{1\,.\,3} + \frac{1}{3\,.\,5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$

e. $n^2 \leq 2^n, \quad n \geq 4$

4. Pruebe por inducción matemática.
   a. $11^n - 6$ es divisible entre 5 para toda $n \geq 1$.
   b. $6 \,.\, 7^n - 2 \,.\, 3^n$ es divisible entre 4 para toda $n \geq 1$.
   c. Si n es impar, pruebe que $7^n + 1$ es divisible por 8.
   d. Si n es par, pruebe que $5^n - 1$ es divisible por 8.

Recursión

La recursión es una técnica muy poderosa, utilizada con mucha frecuencia en ciencias computacionales y que facilita soluciones simples a problemas de cierta complejidad. **Recursión o recursividad** es el proceso en que un objeto de define en término de si mismo. Es decir cuando el objeto se define en término de valores previos del mismo objeto. Todo proceso recursivo genera una sucesión. En ocasiones, los términos de una sucesión se puede dar recursivamnete, siempre que se definan los primeros términos de la sucesión y se de una fórmula para calcular los demás en término de los anteriores. Por ejemplo, la definición de $n!$ es recursiva, porque $n!$ de define en término de valores anteriores de si mismo.

Otro ejemplo es la sucesión de Fibonacci, definida como

$$F_n = F_{n-1} + F_{n-2},\ n = 3, 4, \ldots,\ F_1 = 1,\ F_2 = 1.$$

En este caso, el objeto de define en término de dos valores previos del mismo objeto.

En todo proceso recursivo, se requiere de dos pasos:

a. **Paso base:** es el paso donde se especifica el conjunto de los primeros valores o valores iniciales del objeto.
b. **Paso recursivo:** es el paso donde se definen los demás valores del objeto en término de los valores previos.

En el caso del $n!$ el paso base es $0! = 1$ y el paso recursivo es $n(n-1)!$. En la sucesión de Fibonacci, el paso base está formado por

$$F(1) = 1, \qquad F(2) = 1$$

y el paso recursivo por

$$F(i) = F(i-1) + F(i-2),\ i = 3, 4, 5, \ldots, .$$

Todo proceso recursivo debe conducir al paso base; de lo contrario puede haber problemas para la solución del problema que trata de resolverse. De aquí la importancia de analizar profundamente la implementación recursiva de la solución de un problema.

La recursión se puede presentar de varias maneras:

a. **Directa:** Esta ocurre cuando el objeto se define en término de si mismo.

b. **Indirecta:** Se presenta cuando el objeto de define en término de otro objeto, el cual a su vez de define en término del primero.

En términos computacionales, algunos lenguajes de programación permiten la recursión, otros no. Utilice recursividad si conoce perfectamente lo que está haciendo; en caso contrario, utilice la iteratividad. En algoritmos computacionales se estudia a profundidad la pertinencia de la iteratividad y la recursividad.

Por ejemplo, el siguiente código muestra una implementación recursiva para calcular $n!$. Suponga que n es un número natural.

```
factorial_rec(n)
Si n = 0
   entonces
    factorial_rec = 1;     \\paso base
   si no
    factorial_rec = n * factorial_rec (n - 1);\\p. rec
Fin del Si
```

Una expresión matemática para el código anterior es la siguiente

$$f(n) = \begin{cases} 1, & n = 0 \\ n\, f(n-1), & n > 0 \end{cases}.$$

Por ejemplo, si queremos calcular $f(5)$, tenemos que

$$\begin{aligned}
f(5) &= 5 \times f(4) = 5 \times 24 = 120 \\
f(4) &= 4 \times f(3) = 4 \times 6 = 24 \\
f(3) &= 3 \times f(2) = 3 \times 2 = 6 \\
f(2) &= 2 \times f(1) = 2 \times 1 = 2 \\
f(1) &= 1 \times f(0) = 1 \times 1 = 1
\end{aligned}$$

Luego,

$$f(5) = 120.$$

Ejemplo

Consideremos la función recursiva definida por;

$$f(n) = \begin{cases} 0, & n = 0 \\ 2\,f(n-1) + n^3 + 1, & n > 0 \end{cases}.$$

Para calcular $f(4)$, tenemos que:

$$\begin{aligned}
f(4) &= 2f(3) + 4^3 + 1 = 2(54) + 64 + 1 = 173 \\
f(3) &= 2f(2) + 3^3 + 1 = 2(13) + 27 + 1 = 54 \\
f(2) &= 2f(1) + 2^3 + 1 = 2(2) + 8 + 1 = 13 \\
f(1) &= 2f(0) + 1^3 + 1 = 2
\end{aligned}$$

Luego,

$$f(4) = 173.$$

Una implementación iterativa para calcular $n!$ sería como sigue:

Suponga que n es un número natural y `nfact` es una variable tipo entera.

```
factorial_ite(n)
    nfact = 1;
    Mientras (n > 0 )
        nfact = n * nfact;
        n = n - 1;
    Fin del Mientras
    Escribir nfact;
```

Se puede probar fácilmente que el orden de complejidad de ambas implementaciones es la misma. Sin embargo, en el caso de la sucesión de Fibonacci, la situación es muy diferente, ya que la implementación recursiva tiene un orden de complejidad exponencial (ineficiente e impráctica), mientras que la implementación iterativa tiene una complejidad lineal, lo que la hace mucho más eficiente.

1. si $f(n) = \begin{cases} 1, & n \leq 1 \\ 2\,f(n-1)+1, & n > 1 \end{cases}$. Encuentre $f(5)$.
2. si $f(n) = \begin{cases} 1, & n \leq 1 \\ f(n/2)+1, & n > 1 \end{cases}$. Encuentre $f(15)$.
3. si $f(n) = \begin{cases} 1, & n = 0 \\ n + f(n-1)+1, & n > 0 \end{cases}$. Encuentre $f(6)$.
4. si $f(n) = \begin{cases} 1, & n = 1 \\ 2\,f(n-1)+n, & n > 1 \end{cases}$. Encuentre $f(8)$.
5. Si $f(n) = \begin{cases} 5, & n = 1 \\ 5\,f(n-1), & n > 1 \end{cases}$. Encuentre $f(4)$.

Ejercicios

6. Si $f(n) = \begin{cases} 1, & n = 1 \\ n + f(n-1), & n > 1 \end{cases}$. Encuentre $f(5)$.
7. Si $f(n) = \begin{cases} 7, & n = 0 \\ f(n-1) + 1, & n > 0 \end{cases}$. Encuentre $f(6)$.
8. Si $f(n) = \begin{cases} n, & n < 2 \\ f(n-1) + f(n-2), & n \geq 2 \end{cases}$. Encuentre $f(5)$.
9. Si $f(m, n) = \begin{cases} m, & n = 0 \\ f(n, m \,\%\, n), & n > 0 \end{cases}$. Encuentre $f(45, 18)$.
10. Si $f(m, n) = \begin{cases} m, & n = 1 \\ m\, f(m, n-1), & n > 1 \end{cases}$. Encuentre $f(7, 4)$.

Ejercicios

11. Si $f(m,n) = \begin{cases} m, & n=0 \\ f(m,n-1)+1, & n>0 \end{cases}$. Encuentre $f(5,6)$.
12. Si $f(m,n) = \begin{cases} m, & n=0 \\ f(m,n-1)+m, & n>0 \end{cases}$. Encuentre $f(6,7)$.
13. Si $f(m,n) = \begin{cases} m, & n=0 \\ f(m,n-1)+n, & n>0 \end{cases}$. Encuentre $f(8,10)$.
14. Si $A(m,n) = \begin{cases} n+1, & m=0 \\ A(m-1,1), & m>0,\ n=0 \\ A(m-1,A(m,n-1)), & m>0,\ n>0 \end{cases}$. Encuentre $A(3,0)$ y $A(2,1)$. Esta es la conocida función de Ackermann.

15. Si $f(m,n) = \begin{cases} 0, & m < n \\ f(m-n,n)+1, & m \geq n \end{cases}$. Encuentre $f(15,4)$.

16. Si $f(n) = \begin{cases} 0, & n = 0 \\ f(n/10)+(n\,\%10), & n > 0 \end{cases}$. Encuentre $f(324)$.

17. Sea v un vector y n un entero no negativo.

    Si $f(v,n) = \begin{cases} v[n], & n = 0 \\ f(v,n-1)+v[n], & n > 0 \end{cases}$.

    Encuentre $f([-1,3,6,9],4)$.

18. Sea v un vector y n un entero no negativo.

    Si $f(v,n) = \begin{cases} v[n], & n = 0 \\ v[n] * f(v, n-1), & n > 0 \end{cases}$.

    Encuentre $f([2,5,3,6,3],5)$.

19. Escriba en seudocódigo una función recursiva que sume dos números enteros.

20. Escriba en seudocódigo una función recursiva que sume los elementos de un arreglo.

21. Escriba en seudocódigo una función recursiva que calcule el MCD de dos enteros.

22. Escriba en seudocódigo una función recursiva que escriba un entero invertido.
23. Escriba en seudocódigo una función recursiva que escriba el término n de la sucesión de Fibonacci.
24. Escriba en seudocódigo una función recursiva que sume los dígitos de un número entero.
25. Escriba en seudocódigo una función recursiva que convierta un entero en base 10 a base 8.
26. Escriba en seudocódigo una función recursiva que encuentre los factores primos de un número entero n.
27. Escriba en seudocódigo una función recursiva que convierta un entero en base 10 a hexadecimal.

28. Escriba en seudocódigo una función recursiva que divida dos enteros por restas sucesivas.
29. Escriba en seudocódigo una función recursiva que multiplique los elementos de un arreglo.
30. Escriba en seudocódigo una función recursiva que eleve un real x al entero $n \geq 0$.
31. Escriba en seudocódigo una función recursiva que determine si un número x es positivo.
32. Escriba en seudocódigo una función recursiva que determine si un número entero es impar.
33. Escriba en seudocódigo una función recursiva que determine el elemento máximo de un arreglo.

34. Escriba en seudocódigo una función recursiva que determine sume los elementos de una matriz.

Contenido

Principio o regla de la suma

Supongamos que se desea realizar un trabajo que requiere de ejecutar una de varias tareas: una primera tarea que puede llevarse a cabo de n_1 maneras o una segunda tarea que se puede realizar de n_2 maneras o una tercera tarea que se puede ejecutar de n_3 maneras; y así sucesivamente, hasta una r-ésima tarea que se puede realizar de n_r maneras, con la condición de que dos tareas no se pueden llevar a cabo al mismo tiempo, entonces el trabajo se puede realizar de $n_1 + n_2 + n_3 + \cdots + n_r$ maneras.

Ejemplo

Suponga que un Dealer de vehículos tiene en venta 15 vehículos Honda, 18 vehículos Toyota y 25 vehículos Ford. Un cliente llega y quiere probar uno de los vehículos. Entonces este cliente tiene $15 + 18 + 25 = 58$ maneras de escoger el vehículo a probar.

Ejemplo

Un estudiante tiene en su biblioteca 11 libros de Matemática, 6 libros de Física y 8 libros de Informática. Un compañero le pide un libro prestado. El estudiante puede seleccionar para prestar al compañero uno cualquiera de los $11 + 6 + 8 = 25$ libros que posee.

Principio o regla del producto

Suponga que para realizar un trabajo, se requiere ejecutar varias tareas. La primera de las cuales puede lograrse de n_1 maneras, la segunda de n_2 maneras, y así sucesivamente, hasta una r-ésima que se puede llevar a cabo de n_r maneras, entonces el trabajo se puede realizar de $n_1\, n_2\, \ldots\, n_r$ maneras.

A esta regla con frecuencia se le llama **Principio fundamental de conteo o principio de selección**.

Ejemplo

Suponga que a un festival bailable en pareja (Hombre–Mujer) se presentan 8 hombres y 12 mujeres. Entonces hay $8 \times 12 = 96$ maneras de seleccionar las parejas.

Ejemplo

Suponga que se desea confeccionar placas de vehículos de 7 caracteres, donde los 3 primeros caracteres deben ser letras y los 4 siguientes, dígitos numéricos. Entonces se pueden construir $26 \times 26 \times 26 \times 10 \times 10 \times 10 \times 10 = 175760000$ placas.

Si no se permite repetición de letras, entonces se pueden construir $26 \times 25 \times 24 \times 10 \times 10 \times 10 \times 10 = 156000000$ placas.

Si no se permite repetición de letras ni de dígitos, entonces se pueden construir $26 \times 25 \times 24 \times 10 \times 9 \times 8 \times 7 = 78624000$ placas.

Si se permite repetición en las letras y éstas deben ser sólo vocales y los dígitos sólo deben ser impares, entonces se pueden construir $5 \times 5 \times 5 \times 5 \times 5 \times 5 \times 5 = 78125$ placas.

Contenido

Definición

Dado un conjunto de n elementos. Cualquier arreglo o disposición de los n elementos se le llama **Permutación** de los n elementos del conjunto. Por ejemplo, si se tiene el conjunto $A = \{1, 2, 3\}$, entonces hay 6 diferentes maneras (permutaciones) de arreglar los elementos de A que son:

$$123, \quad 132, \quad 213, \quad 231, \quad 312, \quad 321.$$

Si en cambio, se quiere ordenar dos elementos cada vez, entonces hay 6 maneras diferentes de hacerlo como son:

$$12, \quad 21, \quad 13, \quad 31, \quad 23, \quad 32.$$

Dado un conjunto de n elementos y r un entero, tal que $1 \leq r \leq n$. Entonces el número de disposiciones o permutaciones de tamaño r (tomados r a la vez) para los n elementos del conjunto y según la regla del producto, viene dado por

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1).$$

Ahora bien, podemos escribir la expresión anterior como:

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1) =$$

$$\frac{n(n-1)(n-2)\cdots(n-r+1)(n-r)(n-r-1)\cdots 3\cdot 2\cdot 1}{(n-r)(n-r-1)(n-r-2)\cdots 3\cdot 2\cdot 1} = \frac{n!}{(n-r)!}$$

Observemos que para $r = 0$, se tiene que

$$P(n, 0) = \frac{n!}{(n-0)!} = \frac{n!}{n!} = 1.$$

Así que

$$P(n, r) = \frac{n!}{(n-r)!}, \quad 0 \leq r \leq n.$$

Si se desea encontrar la cantidad de disposiciones de tamaño $(r = n)$ para los n elementos, entonces

$$P(n, r) = P(n, n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!.$$

Permutaciones

En caso de permitir repeticiones de los elementos en las disposiciones, se tiene que hay n^r disposiciones.

Nota.

Si $r < n$ a las permutaciones $P(n, r)$ se le suele llamar **Variaciones** y se representan como $V(n, r)$. Es decir, que $V(n, r) = P(n, r)$ cuando $r < n$.

Ejemplo

a. Sea $A = \{a\}$. El número de permutaciones de un (1) elemento viene dado por $P(n, 1) = P(1, 1) = 1$. Esta es a.
b. Sea $A = \{a, b\}$. El número de permutaciones de dos (2) elementos viene dado por $P(n, 2) = P(2, 2) = 2$. Estas son: ab, ba.

c. Sea $A = \{a, b, c\}$. El número de permutaciones de tres (3) elementos viene dado por $P(n, 3) = P(3, 3) = 6$. Estas son:

$$abc, acb, bac, bca, cab, cba$$

De la misma forma se puede obtener las permutaciones de cuatro o más elementos.

Ejemplo

La cantidad de palabras de 3 letras (variaciones) que se pueden construir, asumiendo que no se permiten repetición de letras viene dada por el número

$V(26, 3) = P(26, 3) = 26 \times 25 \times 24 =$

$$\frac{26 \times 25 \times 24 \times \cdots \times 3 \times 2 \times 1}{23 \times 22 \times 21 \times \cdots \times 3 \times 2 \times 1} = \frac{26!}{(26-3)!} = 15600.$$

Ejemplo

El número de permutaciones de tamaño 5 que pueden tenerse con las letras de la palabra "BYTES" es

$$P(5,5) = \frac{5!}{(5-5)!} = \frac{5!}{0!} = 5!.$$

Si las palabras fueran de tamaño 3, entonces el número de permutaciones (variaciones) es

$$V(5,3) = P(5,3) = \frac{5!}{(5-3)!} = \frac{5!}{2!} = 60.$$

Si se permite repeticiones de letras y queremos encontrar la cantidad de permutaciones de tamaño 7. Entonces el número de permutaciones viene dado por

$$5^7.$$

Esto así porque las permutaciones tienen la forma $xxxxxxx$ y cada posición x tiene 5 posibilidades. Luego, se aplica la regla del producto para obtener el resultado anterior.

Ejemplo

Una compañía constructora de semáforos, tiene 5 tonalidades para el color rojo, 8 tonalidades para el color verde y 4 tonalidades para el

color amarillo. ¿Cuántos semáforos diferentes, según sus tonalidades puede construir la compañía?.

Solución

La cantidad de semáforos diferentes es $5 \times 8 \times 4 = 160$.

Consideremos el caso de que se quiere encontrar la cantidad de permutaciones que se pueden construir con las letras de la palabra "$CASA$". Supongamos que las letras "A" son diferentes y diferenciémoslas como A_1 y A_2. Así que la palabra será "CA_1SA_2". Las diferentes permutaciones son :

1.	$A_1\ A_2\ C\ S$ ①	13.	$C\ A_1\ A_2\ S$ ⑦
2.	$A_1\ A_2\ S\ C$ ②	14.	$C\ A_1\ S\ A2$ ⑧
3.	$A_1\ C\ A_2\ S$ ③	15.	$C\ A_2\ A_1\ S$ ⑦
4.	$A_1\ C\ S\ A_2$ ④	16.	$C\ A_2\ S\ A_1$ ⑧
5.	$A_1\ S\ A_2\ C$ ⑤	17.	$C\ S\ A_2\ A_1$ ⑨
6.	$A_1\ S\ C\ A_2$ ⑥	18.	$C\ S\ A_1\ A_2$ ⑨
7.	$A_2\ A_1\ C\ S$ ①	19.	$S\ C\ A_1\ A_2$ ⑩
8.	$A_2\ A_1\ S\ C$ ②	20.	$S\ C\ A_2\ A_1$ ⑩
9.	$A_2\ C\ A_1\ S$ ③	21.	$S\ A_2\ C\ A_1$ ⑪
10.	$A_2\ C\ S\ A_1$ ④	22.	$S\ A_2\ A_1\ C$ ⑫
11.	$A_2\ S\ C\ A_1$ ⑥	23.	$S\ A_1\ A_2\ C$ ⑫
12.	$A_2\ S\ A_1\ C$ ⑤	24.	$S\ A_1\ C\ A_2$ ⑪

Las permutaciones que tienen el mismo número dentro del círculo se consideran las mismas, si A_1 y A_2 son la misma letra (A). Esto indica

que hay 12 permutaciones y se debe a que la letra A aparece $2! = 2 \times 1$ veces en la palabra "$CASA$".

Supongamos ahora que dentro de los n elementos del conjunto, hay n_1 iguales, n_2 iguales, n_3 iguales, y así sucesivamente, hasta n_r iguales, de modo tal que $n_1 + n_2 + n_3 + \cdots + n_r = n$. En estas condiciones la cantidad de permutaciones de los n elementos viene dada por

$$\frac{n!}{n_1!n_2!n_3!\cdots n_r!}.$$

Ejemplo

El número de permutaciones que pueden obtenerse con las letras de la palabra “CABALLO” es

$$\frac{7!}{1!2!1!2!1!} = 1260.$$

1. ¿De cuántas formas pueden ordenarse los símbolos a, b, c, d, e?
2. ¿De cuántas formas pueden ordenarse las letras de la palabra "ANACAONA"?.
3. ¿Cuántas disposiciones hay donde las "A" de la palabra "ANACAONA" aparecen juntas?
4. ¿De cuántas formas pueden ordenarse los símbolos $x, y, z, w, t, t, t, t, t$ de modo que ninguna t sea adyacente a otra?.

5. Determine el número de enteros de seis dígitos (que no empiecen con cero) de modo tal que:
   a. No se repita ningún dígito.
   b. Se puedan repetir dígitos.
   c. No se repita ningún dígito y que sea par.
   d. Se puedan repetir dígitos y que sea par.
   e. No se repita ningún dígito y sea divisible por 4.
   f. Se puedan repetir dígitos y sea divisible por 5 o 3.

6. Encuentre el o los valores de n en las siguientes expresiones:
   a. $P(n, 2) = 90$, b. $P(n, 3) = 3P(n, 2))$, c. $2P(n, 2) + 50 = P(2n, 2)$
7. Sean n y k enteros no negativos. Sea $n + 1 > k$. Demuestre que

$$P(n+1, k) = \left(\frac{n+1}{n+1-k}\right) P(n, k).$$

8. Considere el siguiente segmento de programa:

```
for (i = 1; i <= 12; i++)
     for (j = 5; j <= 10; j++)
          for (k = 15; k >= 8; k--)
               printf("\n, %d",(i-j)*k);
```

¿Cuántas veces se ejecuta la proposición "`printf`"?.

9. ¿Cuántas permutaciones pueden construirse con las letras de la palabra “BIOLOGICA”?
10. ¿En cuántas permutaciones son adyacentes la “A” y la “G” de la palabra del item 9?
11. ¿En cuántas permutaciones son adyacentes todas las vocales?

12. Suponga que hay 4 líneas de transporte entre las paradas A y B y 3 líneas entre B y C.
    a. ¿De cuántas maneras puede una persona viajar de A a C pasando por B?.
    b. ¿De cuántas maneras puede una persona hacer el viaje de ida y regreso de A a C pasando por B?.
    c. ¿De cuántas maneras puede una persona hacer el viaje redondo de A a C pasando por B, si no desea usar la misma línea de transporte más de una vez?.

13. Si no se permiten repeticiones, entonces
    a. ¿Cuántos números de tres dígitos puede formarse a partir de los dígitos 2, 3, 5, 6, 7, 9?.
    b. ¿Cuántos de los números del item a. son menors de 400?.
    c. ¿Cuántos de los números del item a. son pares?.
    d. ¿Cuántos de los números del item a. son impares?.
    e. ¿Cuántos de los números del item a. son múltiplos de 5?.
14. Resuelva el ejercicio 13, asumiendo que se permiten repeticiones

15. ¿De cuántas maneras puede organizarse una grupo de 7 personas :
    a. En una fila de 7 asientos
    b. Alrededor de una mesa redonda
16. ¿De cuántas maneras pueden sentarse 3 niños y 2 niñas en una fila?. ¿De cuántas maneras pueden ellos sentarse en una fila si los niños y las niñas deben sentarse juntos?. ¿De cuántas maneras pueden sentarse en una fila si solamente las niñas deben sentarse juntas?.

17. ¿Cuántas señales diferentes, cada una consistente de 8 banderas colgadas en una línea vertical, pueden formarse con 5 banderas rojas idénticas y con 3 banderas azules idénticas?.
18. Un byte es una secuencias de 8 bits adyacentes y considerado como unidad. ¿Cuántos bytes diferentes se pueden formar?

19. ¿De cuántas maneras se pueden sentar en una filas 3 dominicanos, 4 españoles, 4 haitianos y 2 colombianos de manera que todos los de la misma nacionalidad se sienten juntos?.
20. Suponga que una urna contiene 8 bolas. Encontrar el número de muestras ordenadas de magnitud 3 con reposición. Resolver el mismo problema, pero sin reposición.

21. ¿Cuántas selecciones distintas de presidente y vicepresidente se pueden hacer de un club de 25 miembros?.
22. Si de los 25 miembros, hay 15 hombres y 10 mujeres, ¿cuántas selecciones distintas hay con la condición de que el presidente y vicepresidente sean de distinto sexo?.
23. Sea $A = \{1, 3, 5, 7\}$. Construya todas las permutaciones sin repetición de tamaño 3.
24. Sea $A = \{a, e, i, o, u\}$. Construya todas las disposiciones sin repetición de tamaño 2.

25. Sea $A = \{a, b, c, d\}$. Construya todas las permutaciones con repetición de tamaño 2.
26. Sea $A = \{a, b\}$. Construya todas las permutaciones con repetición de tamaño 4.
27. Sea $A = \{a, b, c\}$. Construya todas las permutaciones con repetición de tamaño 3.
28. ¿De cuántas maneras se pueden repartir 7 juguetes entre 3 niños, si el menor recibe 3 juguetes y los otros reciben 2 cada uno?.

29. En una clase hay 12 estudiantes. ¿De cuántas maneras pueden los 12 estudiantes tomar 3 exámenes diferentes, si 4 estudiantes deben tomar cada examen?.
30. ¿De cuántas maneras se pueden repartir 12 estudiantes en 3 equipos, de modo que cada equipo contenga 4 estudiantes?.

Contenido

Combinaciones

Dado un conjunto de n objetos y $0 \leq r \leq n$. El numero de selecciones o combinaciones de tamaño r (se toman r a la vez) de los n objetos dados, donde el orden carece de importancia, se define por

$$C(n, r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Ejemplo

Sea $A = \{1, 2, 3\}$. El número de combinaciones tomadas de 2 en 2 $(r = 2)$ de los 3 objetos del conjunto A, viene dado por

$$C(3, 2) = \binom{3}{2} = \frac{3!}{2!(3-2)!} = \frac{3!}{2!1!} = 3.$$

Observe que 12 es lo mismo que 21. Así que las combinaciones son :

$$12, \quad 13, \quad 23.$$

Ejemplo

Sea $A = \{a, b, c, d\}$.

a. ¿Cuántas combinaciones sin repetición de un (1) elemento ($r = 1$) se pueden construir?. Se pueden construir

$$C(4,1) = \binom{4}{1} = \frac{4!}{1!(4-1)!} = 4$$

combinaciones. Estas son

$$a, b, c, d$$

b. ¿Cuántas combinaciones sin repetición de dos (2) elementos ($r = 2$) se pueden construir?. Se pueden construir

$$C(4,2) = \binom{4}{2} = \frac{4!}{2!(4-2)!} = 6$$

combinaciones. Estas son

$$ab, ac, ad, bc, bd, cd$$

c. ¿Cuántas combinaciones sin repetición de tres (3) elementos ($r = 3$) se pueden construir?. Se pueden construir

$$C(4,3) = \binom{4}{3} = \frac{4!}{3!(4-3)!} = 4$$

combinaciones. Estas son

$$abc, abd, acd, bcd$$

d. ¿Cuántas combinaciones sin repetición de cuatro (4) elementos ($r = 4$) se pueden construir?. Se pueden construir

$$C(4,4) = \binom{4}{4} = \frac{4!}{4!(4-4)!} = 1$$

combinación. Esta es

$$abcd$$

Observemos que se trata de combinaciones sin repetición, por lo que no se puede seguir construyendo combinaciones de 5 o más elementos.

Ejemplo

El manager de un equipo de Beisbol tiene 26 peloteros disponibles para el juego, pero sólo debe seleccionar 9. ¿De cuántas maneras puede el Manager seleccionar el equipo de juego?.

Solución

Hay $C(26,9) = \binom{26}{9} = \frac{26!}{9!(26-9)!} = 3124550$ maneras de seleccionar el equipo.

Ejemplo

Un estudiante toma un examen de sociología que contiene 10 preguntas de las cuales debe responder 7. ¿De cuántas maneras puede responder el estudiante el examen?.

Solución

Como el orden no tiene importancia, se tiene que el estudiante puede responder el examen de

$$C(10,7) = \binom{10}{7} = \frac{10!}{7!3!} = 120$$

maneras.

Combinaciones sin repetición

Si el estudiante debe responder 4 preguntas de las 5 primeras y 3 de las últimas 5, entonces la solución es

$$C(5,4) = \binom{5}{4} = \frac{5!}{4!1!} = 5$$

maneras de responder las primeras cuatro preguntas y

$$C(5,3) = \binom{5}{3} = \frac{5!}{3!2!} = 10$$

maneras de responder las restantes tres preguntas. De modo que aplicando la regla del producto, el estudiante puede responder las 7 preguntas de

$$C(5,4)C(5,3) = \binom{5}{4}\binom{5}{3} = 5 \times 10 = 50$$

maneras.

Ejemplo

Los jugadores de Dominó del Club cabuya son 32. Se prepara un campeonato con 4 equipos de 8 jugadores cada uno. ¿De cuántas maneras se pueden seleccionar los 4 equipos?.

Solución

El primer equipo se puede seleccionar de

$$C(32,8) = \binom{32}{8} = \frac{32!}{8!24!} = 10518300$$

maneras.

El segundo equipo se puede seleccionar de

$$C(24,8) = \binom{24}{8} = \frac{24!}{8!16!} = 735471$$

maneras.

El tercer equipo se puede seleccionar de

$$C(16,8) = \binom{16}{8} = \frac{16!}{8!8!} = 12870$$

maneras.

El cuarto equipo se puede seleccionar de

$$C(8,8) = \binom{8}{8} = \frac{8!}{8!0!} = 1$$

maneras.

Ahora aplicando la regla del producto, se tiene que los cuatro equipos de pueden formar de

$$\begin{aligned} C(32,8)C(24,8)C(16,8)C(8,8) &= \binom{32}{8}\binom{24}{8}\binom{16}{8}\binom{8}{8} \\ &= 10518300 \times 735471 \times 12870 \times 1 \\ &= 9.9561092450391 \times 10^{16} \end{aligned}$$

maneras.

Teorema del binomio (Coeficiente binomial)

Sean a y b dos variables y n un entero positivo. Entonces

$$\begin{aligned}(a+b)^n &= \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \cdots + \\ &\quad + \binom{n}{n-1}a^1 b^{n-1} + \binom{n}{n}a^0 b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \\ &= \sum_{k=0}^{n}\binom{n}{n-k}a^{n-k}b^k\end{aligned}$$

Ejemplo

Determinar el coeficiente del término a^3b^4 en el desarrollo de $(2a+b^2)^5$.

Solución

El coeficiente es :

$$\binom{5}{2}(2)^3(1)^2 = \binom{5}{3}(2)^3(1)^2 = \frac{5!}{3!2!}(2)^3(1)^2 = 80.$$

Otra forma

Sabemos que el término general de a^3b^4 es

$$\binom{5}{k}(2a)^{5-k}(b^2)^k = \binom{5}{k}2^{5-k}a^{5-k}b^{2k}.$$

De donde

$$a^{5-k}b^{2k} = a^3b^4.$$

Luego, $k = 2$ y el coeficiente es

$$\binom{5}{2}(2)^3 = \frac{5!}{2!3!}(8) = 80.$$

Teorema del coeficiente multinomial

Sean n y r enteros positivos. Entonces el desarrollo de $(x_1 + x_2 + x_3 + \cdots + x_r)^n$ tiene como coeficiente de

$$x_1^{n_1}x_2^{n_2}x_3^{n_3}\cdots x_r^{n_r}$$

la cantidad de

$$\binom{n}{n_1, n_2, n_3, \cdots, n_r} = \frac{n!}{n_1! n_2! n_3! \cdots n_r!},$$

donde los n_i son enteros, tales que

$$0 \leq n_i \leq n, \quad i = 1, 2, \cdots, r \text{ y } n_1 + n_2 + n_3 + \cdots + n_r = n.$$

La suma de los coeficientes multinomiales viene dada por la fórmula

$$\sum_{n_1+n_2+\cdots+n_r=n} \binom{n}{n_1, n_2, n_3, \cdots, n_r} = r^n.$$

Por ejemplo, la suma de los coeficientes en el desarrollo de $(a+b+c)^5$ es $r^n = 3^5 = 243$. La cantidad de términos en el desarrollo de

$$(x_1 + x_2 + \cdots + x_r)^n,$$

viene dada por la expresión

$$CM(n,r) = \binom{n+r-1}{n} = \binom{n+r-1}{r-1}.$$

Por ejemplo, la cantidad de términos en el desarrollo de $(a+b+c)^5$ es

$$CM(n,r) = CM(5,3) = \binom{7}{5} = \binom{7}{2} = 21.$$

1. Sea $A = \{a, b, c, d, e\}$. Construya todas la combinaciones sin repetición de tamaño 3.
2. Sea $A = \{a, b, c, d, e, f\}$. Construya todas la combinaciones sin repetición de tamaño 4.
3. Sea $A = \{1, 2, 3, 4\}$. Construya todas la combinaciones sin repetición de tamaño 3. Obtenga las permutaciones para cada una de las combinaciones y deduzca la relación que hay con las permutaciones de tamaño 3 de un conjunto de 4 elementos, $P(4, 3)$.
4. En una reunión familiar hay 5 hombres y 6 mujeres. Cuatro de las personas van al supermercado a comprar los ingredientes de un Sancocho.

a. ¿De cuántas maneras se pueden seleccionar las 4 personas que van al supermercado?.
b. ¿De cuántas maneras se pueden seleccionar las 4 personas que van al supermercado, si tienen que ir 2 hombres y 2 mujeres?.

5. La directiva de la junta de vecinos del barrio Cuernavaca formada por 14 miembros, ofrece un agasajo a 9 de sus miembros. ¿De cuántas formas puede seleccionar los 9 miembros?.
6. Demuestre que
$$\binom{n}{k} = \binom{n}{n-k}$$
7. Demuestre que:
   a. $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$

b. $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$

c. $\binom{2n}{n} + \binom{2n}{n-1} = \frac{1}{2}\binom{2n+2}{n+1}, \quad n \in \mathbb{Z}^+$

d. $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$

e. $\binom{n}{n_1, n_2} = \binom{n}{n_1} = \binom{n}{n_2}$

8. Se selecciona un comité de 12 personas de un grupo de 10 hombres y 10 mujeres. ¿De cuántas maneras se puede realizar la selección, si:
   a. no hay restricciones.
   b. debe haber 6 hombres y 6 mujeres

c. debe haber un número par de mujeres
d. debe haber más mujeres que hombres
e. debe haber ocho hombres como mínimo

9. ¿De cuántas maneras se puede seleccionar un equipo de baloncesto de 5 personas de entre 12 jugadores posibles?.¿Cuántas selecciones incluyen al más débil y al más fuerte de los jugadores?.
10. ¿De cuántas maneras se pueden distribuir 12 libros distintos entre 4 niñosde modo que:
    a. cada niño recibe tres libros.
    b. los dos niños mayores reciban 4 libros cada uno y los dos menores 2 cada uno.

11. ¿Cuántas permutaciones de las letras de la palabra "MISSISSIPPI" no tienen "S" consecutivas?.
12. ¿Cuántos triángulos determinan los vértices de un polígono regular de n lados?. ¿Cuántos, si ningún lado del polígono se usa como lado del triángulo?.
13. Determine el coeficiente de x^9y^3 en: a. $(x+y)^{12}$, b. $(x+2y)^{12}$, c. $(2x+3y)^{12}$
14. Determine el coeficiente de xyz^2 en $(x+y+z)^4$, en $(2x-y-z)^4$ y en $(w+x+y+z)^4$.
15. Determine el coeficiente de $w^3x^2yz^2$ en $(2w-x+3y-2z)^8$.

16. Determine la suma de todos los coeficientes de:

    a. $(x+y)^3$ b. $(x+y)^{10}$ c. $(x+y+z)^{10}$
    d. $(w+x+y+z)^5$ b. $(x-y)^{10}$ c. $(2x-3y+z)^{10}$

17. ¿De cuántas maneras puede formarse un equipo que consta de 4 hombres y 3 mujeres, de un grupo de 8 hombres y 6 mujeres?.

18. Suponga que dentro de una funda hay 6 bolas blancas y 5 bolas negras. Encuentre el número de maneras en que se pueden sacar 4 bolas de la funda.

    a. si pueden ser de cualquier color.
    b. si 2 deben ser blancas y 2 deben ser negras.
    c. todas deben ser del mismo color.

19. Suponga que hay 12 puntos $A, B, C, \ldots$ en un plano dado, donde no hay 3 puntos sobre la misma recta.

a. ¿Cuántas líneas se pueden construir sobre los puntos?.
b. ¿Cuántas de las líneas pasan por el punto A?.
c. ¿Cuántos triángulos se pueden construir con los puntos?.
d. ¿Cuántos de los triángulos contienen el punto A como vértice?.

20. Un estudiante debe responder 8 de 10 preguntas en un examen.
    a. ¿Cuántas posibilidades tiene?.
    b. ¿Cuántas posibilidades tiene, si debe responder las primeras 3 preguntas?.
    c. ¿Cuántas posibilidades tiene, si tiene que responder por lo menos 4 de las primeras 5 preguntas?.
21. ¿Cuántas diagonales tiene un octógono?
22. ¿Cuántas diagonales tiene un polígono regular de n lados?

Ejercicios

23. ¿Qué polígono regular tiene el mismo número de diagonales que de lados?
24. ¿Cuántos comités de 5 personas con un director dado, pueden formarse a partir de 12 personas?
25. Encuentre el número de subconjuntos de un conjunto A que contiene n elementos.
26. ¿De cuántas maneras se puede escoger uno o más estudiantes a partir de 6 que son elegibles?.
27. ¿De cuántas maneras puede escogerse 3 o más estudiantes a partir de 12 que son elegibles?.
28. ¿Qué polígono regular tiene 90 diagonales?

Contenido

Dado un conjunto de n elementos, de los cuales se desea seleccionar con repetición, r elementos. El número de combinaciones con repetición de n elementos, tomados de r en r, viene dado por

$$C(n+r-1,r)=\binom{n+r-1}{r}=\frac{(n+r-1)!}{r!(n-1)!}.$$

Observe que en este caso, puede ocurrir que $r \geq n$.

Ejemplo

Sea $A=\{a,b,c,d\}$.

a. ¿Cuántas combinaciones con repetición de un (1) elemento ($r = 1$) se pueden construir?. Se pueden construir $C(4+1-1,1) = \binom{4}{1} = 4$ combinaciones. Estas son

$$a, b, c, d$$

b. ¿Cuántas combinaciones con repetición de dos (2) elementos ($r = 2$) se pueden construir?. Se pueden construir $C(4+2-1,2) = \binom{5}{2} = 10$ combinaciones. Estas son:

$$aa, ab, ac, ad, bb, bc, bd, cc, cd, dd$$

c. ¿Cuántas combinaciones con repetición de tres (3) elementos ($r = 3$) se pueden construir?. Se pueden construir $C(4+3-1,3) = \binom{6}{3} = 20$ combinaciones. Estas son:

$$aaa, aab, aac, aad, abb, abc, abd, acc, acd, add,$$

$$bbb, bbc, bbd, bcc, bcd, bdd, ccc, ccd, cdd, ddd$$

Se puede seguir construyendo combinaciones de cuatro o más elementos siguiendo el mismo procedimiento.

Ejemplo

Suponga que una librería especializada en Ciencia y Tecnología tiene disponible 27 tipos diferentes de libros. En la librería hay al menos 15 libros de cada tipo. Un Político que desea entregar a estudiantes de su comunidad algunos libros, llega a la librería. El político puede seleccionar 15 libros de

$$C(27+15-1,15) = C(41,15) = \binom{41}{15} = \frac{41!}{15!(41-15)!} = \frac{41!}{15!26!} = 63432274896$$

maneras.

Ejemplo

Un Supermercado decide un día distribuir 12 libras de arroz y 10 libras de habichuelas a 7 familias del vecindario, con la condición de entregar al menos una libra de arroz a cada familia. ¿De cuántas maneras se pueden distribuir el arroz y las habichuelas?.

Solución

Como a cada familia se le entregará una libra de arroz, las libras restantes de pueden distribuir de

$$C(7+5-1,5) = C(11,5) = 462 \text{ maneras.}$$

Las libras de habichuelas se pueden distribuir de

$$C(7+10-1,10) = C(16,10) = 8008 \text{ maneras.}$$

Aplicando la regla del producto, tenemos que el arroz y las habichuelas se pueden distribuir de

$$462 \times 8008 = 3699696 \text{ maneras.}$$

Ejemplo

¿De cuántas maneras se puede distribuir 12 mangos entre 5 personas?.

Solución

Es claro que se trata de un problema de seleccion de tamaño 12 con repetición para una colección de 5. Entonces hay

$$C(5+12-1,12) = C(16,12) = \binom{16}{12} = \frac{16!}{12!4!} = 1820$$

maneras de hacer la distribución.

Observe que este problema es equivalente a encontrar todas las soluciones posibles enteras no negativas de las ecuación

$$x_1 + x_2 + x_3 + x_4 + x_5 = 12, \;\; x_i \in \mathbb{Z}, \;\; x_i \geq 0, \;\; i = 1, 2, 3, 4, 5.$$

1. ¿De cuántas formas se pueden distribuir 10 bolas idénticas entre 6 personas ?
2. ¿De cuántas formas se pueden distribuir 12 monedas (idénticas) entre cinco niños:
   a. si no hay restricciones.
   b. si cada niño recibe una moneda como mínimo.
   c. si el niño mayor obtiene al menos dos monedas.

3 ¿De cuántas formas se pueden distribuir 15 caramelos (idénticos) entre cinco niños, de modoque el menor obtenga sólo uno o dos?.

4 Determine el número de soluciones enteras de $x_1 + x_2 + x_3 + x_4 = 32$, donde

a. $x_i \geq 0, \ \ 1 \leq i \leq 4$.
b. $x_i > 0, \ \ 1 \leq i \leq 4$.
c. $x_1, x_2 \geq 5, \ \ x_3, x_4 \geq 7$.
d. $x_i \geq 8, \ \ 1 \leq i \leq 4$.
e. $x_i \geq -2, \ \ 1 \leq i \leq 4$.
f. $x_1, x_2, x_3 > 0, \ \ 0 < x_4 \leq 25$.

5. Determine el número de soluciones enteras para $x_1 + x_2 + x_3 + x_4 + x_5 < 40$, donde

a. $x_i \geq 0, \ \ 1 \leq i \leq 5$.
b. $x_i \geq -3, \ \ 1 \leq i \leq 5$.

6. ¿De cuántas maneras se pueden distribuir 8 pelatas blancas idénticas en 4 recipientes distintos, de modo que:
   a. ningún recipiente quede vacío?.
   b. que el cuarto recipiente contenga un impar de pelotas?.

7. Halle el coeficiente de v^2w^4xz en $(3v + 2w + x + y + z)^8$.
8. ¿Cuántos términos distintos tiene la expansión del item 7.
9. ¿Cuántas maneras hay de colocar 12 bolas del mismo tamaño en 5 recipientes distintos:
   a. si todas las bolas son negras?.
   b. si cada bola es de diferente color?.
10. Halle el número de soluciones enteras no negativas para $2x_1 + x_2 + x_3 + x_4 = 10$.
11. ¿De cuántas maneras se pueden colocar 9 libros iguales en 5 estantes?.
12. ¿De cuántas maneras se pueden colocar 5 libros iguales en 9 estantes?.

Contenido

Congruencia

Sea $m \in \mathbb{Z}^+$ y sean a y b dos enteros cualesquiera. Se dice que a es **Congruente** con b módulo m, denotado por $a \equiv b \pmod{m}$, si $m|(a-b)$. Es decir, si $a - b = km$ para algún $k \in \mathbb{Z}$. En otras palabras, si el resto de dividir a y b entre m es el mismo.

Ejemplos

$$9 \equiv 4 \pmod{5}, \qquad 28 \equiv 1 \pmod{9}, \qquad 17 \equiv -7 \pmod{8}$$

La operación $\bmod$ se define de la manera siguiente:

Sean $a, b \in \mathbb{Z}^+$. Entonces $a \bmod b$ se define como el resto de dividir a entre b. Por ejemplo, $12 \bmod 7 = 5$

Observe que en caso de la congruencia, el mód se trata como una relación, mientras que en este último caso, el mód es una operación.

Nota: Otra forma de decir que a es congruente a b módulo m, es diciendo que existe un entero k, tal que $a = b + km$.

El concepto de congruencia es utilizado diariamente en nuestras actividades, como por ejemplo, los días de la semana se cuentan módulo 7; las horas del día módulo 24, etc.

Ejemplo

Suponga que en este instante son las cuatro(4) de la tarde. ¿Qué hora será dentro de 250 horas?.

Solución

Sea x la hora que se busca. Entonces

$$x \equiv 16 + 250 \pmod{24}.$$

De donde se obtiene que

$$x \equiv 2 \pmod{24}.$$

Luego, la hora x buscada es las $2 : 00a.m.$.

Si a y b no son congruentes módulo m, se dice que son **Incongruentes** y se escribe $a \not\equiv b \pmod{m}$.

Propiedades de las congruencias

Suponer que m es un entero positivo fijo.

1. Si $a \equiv b \pmod{m}$ y $c \in \mathbb{Z}$, entonces:
   a. $a + c \equiv b + c \pmod{m}$

      Demostración

      Como $a \equiv b \pmod{m}$, se tiene que $m \mid a - b$. Luego, $m \mid (a + c) - (b + c)$ y por tanto,

      $$a + c \equiv b + c \pmod{m}.$$

   b. $ac \equiv bc \pmod{m}$

      Demostración

      Como $a \equiv b \pmod{m}$, se tiene que $m \mid a - b$ y por tanto, $m \mid (a - b)c$. Luego, $m \mid ac - bc$ y

      $$ac \equiv bc \pmod{m}.$$

Ejemplo

Si $10 \equiv 1 \pmod{9}$, entonces $200 \equiv 20 \pmod{9}$.

Nota: El recíproco del teorema anterior no es cierto en general. Es decir, si $ac \equiv bc \pmod{m}$, no se puede deducir que $a \equiv b \pmod{m}$.

Por ejemplo, $16 \equiv 8 \pmod{8}$. Sin embargo, $8 \not\equiv 4 \pmod{8}$.

2. Si $a, b, c, d \in \mathbb{Z}$ y $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, entonces

a. $a + c \equiv b + d \pmod{m}$

Demostración

Si $a \equiv b \pmod{m}$, existe $k \in \mathbb{Z}$ tal que $a - b = km$. Del mismo modo, si $c \equiv d \pmod{m}$, existe $h \in \mathbb{Z}$ tal que $c - d = hm$. Sumando miembro a miembro ambas ecuaciones, se obtiene

$$(a - b) + (c - d) = (a + c) - (b + d) = (k + h)m,$$

donde $(k + h) \in \mathbb{Z}$. Luego,

$$a + c \equiv b + d \pmod{m}.$$

b. $ac \equiv bd \pmod{m}$

Demostración

Si $a \equiv b \pmod{m}$, existe $k \in \mathbb{Z}$ tal que $a - b = km$. Del mismo modo,si $c \equiv d \pmod{m}$, existe $h \in \mathbb{Z}$ tal que $c - d = hm$. Multiplicando la primera ecuación por c y la segunda por b y sumando miembro a miembro, se obtiene

$$ac - bd = (ck + bh)m,$$

donde $(ck + bh) \in \mathbb{Z}$. Luego,

$$ac \equiv bd \pmod{m}.$$

3. Congruencia de Polinomios.

   Si

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + c_{n-2} x^{n-2} + \cdots + c_1 x + c_0$$

   es un polinomio con coeficientes $c_i \in \mathbb{Z}$, entonces,

   si $a \equiv b \pmod{m}$, se tiene que

$$f(a) \equiv f(b) \pmod{m}.$$

   Demostración

   Como $a \equiv b \pmod{m}$ y aplicando los resultados del item 2, se obtiene

$$a^i \equiv b^i \pmod{m}, 1 \leq i \leq n.$$

Multiplicando por c_i se tiene

$$c_i a^i \equiv c_i b^i \pmod{m}.$$

Sumando todas las ecuaciones obtenemos

$c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0 \equiv c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0 \pmod{m}$.

Luego,

$$f(a) \equiv f(b) \pmod{m}.$$

Teorema

Sean $a, b \in \mathbb{Z}$. Sea k un entero positivo y $d = MCD(k, m)$. Entonces si $ka \equiv kb \pmod{m}$, se tiene que $a \equiv b \pmod{\frac{m}{d}}$

Demostración

Como $ka \equiv kb \pmod{m}$, tenemos que $m \mid k(a-b)$. Luego,

$$\frac{m}{d} \,\Big|\, \frac{k(a-b)}{d}.$$

Como $MCD(\frac{m}{d}, \frac{k}{d}) = 1$, se tiene necesariamente que

$$\frac{m}{d} \,\Big|\, a - b.$$

Por tanto,

$$a \equiv b \left(\text{mód } \frac{m}{d}\right).$$ ■

Ejemplo

Consideremos la congruencia $32 \equiv 24 \,(\text{mód } 8)$.

Es decir, $4 \times 8 \equiv 4 \times 6 \,(\text{mód } 8)$. Como $MCD(4, 8) = 4$, tenemos que

$$8 \equiv 6 \,(\text{mód } 2).$$

Corolario

Sea m primo y k un entero positivo, tal que $MCD(k, m) = 1$. Entonces si

$$ka \equiv kb \pmod{m}, \text{ se tiene que } a \equiv b \pmod{m}.$$

1. Si hoy es Miércoles, ¿qué día de la semana será
   a. dentro de 22 días?
   b. dentro de 150 días?
2. Determine el valor de verdad de las siguientes afirmaciones:
   a. $18 \equiv 1 (\text{mód } 5)$
   b. $86 \equiv 1 (\text{mód } 5)$
   c. $100 \equiv 10 (\text{mód } 9)$
   d. $62 \not\equiv 2 (\text{mód } 8)$
   e. $10^3 \equiv 1 (\text{mód } 9)$
   f. $2a \equiv 6 (\text{mód } 2)$
   g. $s^2 + s + 1 \equiv 2 (\text{mód } 2)$
   h. $a(a+1)(a+2) \equiv 0 (\text{mód } 3)$

3. Si hoy es 27 de Octubre de 1993, ¿qué día de la semana será el 27 de Octubre de 1994?.
4. Construya las tablas para las operaciones de suma y producto módulo 7.
5. Utilizando las tablas anteriores, resuelva las siguientes congruencias
   a. $2a \equiv 3 \pmod{7}$
   a. $5a \equiv 4 \pmod{7}$

Definición

Sea $A = \mathbb{Z}$ y $a \in A$. Se llama **Clase de congruencia** de a módulo m, representada por $[a]$, al conjunto

$$[a] = \{x \in A \,|\, x \equiv a \pmod{m}\} = \{x \in A \,|\, \exists k \in \mathbb{Z},\ x - a = mk\}.$$

Ejemplo

Sea $m = 7$. Algunos casos de muestra son:

$$[0] = \{\dots, -21, -14, -7, 0, 7, 14, 21, 28, \dots\} = \{7k \,|\, k \in \mathbb{Z}\}$$
$$[1] = \{\dots, -20, -13, -6, 1, 8, 15, 22, 29, \dots\} = \{7k + 1 \,|\, k \in \mathbb{Z}\}$$
$$[2] = \{\dots, -19, -12, -5, 2, 9, 16, 23, 30, \dots\} = \{7k + 2 \,|\, k \in \mathbb{Z}\}$$

Si se continua el proceso, observamos que

$$[0] = [7],\ [1] = [8],\ [2] = [9], \ldots.$$

Esto quiere decir que cada entero pertenece exactamente a uno y solo uno de los conjuntos

$$[0],\ [1],\ [2],\ [3],\ [4],\ [5],\ [6].$$

Generalizando, si $s \in \mathbb{Z}$ se tiene que $[s] = [t],\ \ 0 \leq t \leq 6.$
Entonces podemos decir que

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5] \cup [6].$$

Y que todo $s \in \mathbb{Z}$, se puede escribir como

$$s = 7m + t \text{ para algún } m \in \mathbb{Z} \text{ y } 0 \leq t \leq 6.$$

El conjunto

$$\{[0],\ [1],\ [2],\ [3],\ [4],\ [5],\ [6]\}.$$

se representa por $\mathbb{Z}_7$. Se escribe generalmente $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ cuando no hay lugar a confusión. En sentido general, se tiene que

$$\mathbb{Z}_m = \{0, 1, 2, 3, \ldots, m-1\}.$$

A este conjunto se le llama **Enteros módulo** m.

Ahora definamos las operaciones aritméticas básicas ($+$ y $\cdot$) en términos modular (en $\mathbb{Z}_m$) de la siguiente manera:

Sean $a, b \in \mathbb{Z}_m, \;\; m$ entero positivo. Entonces

1. $a + b = a + b \,(\text{mód } m)$
2. $a \,.\, b = a \cdot b \,(\text{mód } m)$

Otra forma de representar las ecuaciones anteriores es escribiendo:

1. $[a] + [b] = [a + b]$
2. $[a] \,.\, [b] = [a \cdot b]$

Es fácil probar que estas operaciones están bien definidas.

Se puede comprobar que $\mathbb{Z}_m$ es cerrado con respecto a estas operaciones.

Además las operaciones satisfacen las siguientes:

Propiedades

Sean $a, b, c \in \mathbb{Z}_m, \quad m \geq 2.$

a. Conmutativa: $a + b = b + a, \;\; a \cdot b = b \cdot a$.
b. Asociativa: $(a + b) + c = a + (b + c), \;\; (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
c. Identidades (Elementos neutros para suma y producto): $a + e = e + a = a, \;\; a \cdot e = e \cdot a = a$.
d. Opuesto e Inverso: $a + a' = a' + a = e, \;\; a \cdot a' = a' \cdot a = e$.

e. Distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Ejemplo

Sea $m = 7$. Entonces

$5 + 4 = 5 + 4 \pmod{7} = 2$
$5 \cdot 4 = 5 \times 4 \pmod{7} = 6.$

Ejemplo

Sea $m = 5$. Entonces

$[36] + [47] = [83] = [3] = \{x \in \mathbb{Z} \mid x = 5k + 3, \quad k \in \mathbb{Z}\} =$
$\{\ldots, -17, -12, -7, -2, 3, 8, 13, \ldots\}$
$[36] \,.\, [47] = [1692] = [2] = \{x \in \mathbb{Z} \mid x = 5k + 2, \quad k \in \mathbb{Z}\} =$
$\{\ldots, -18, -13, -8, -3, 2, 7, 12, \ldots\}$

Prueba de la propiedad c (suma)

Sea $a \in \mathbb{Z}_m$ y sea e el elemento neutro de la suma. Entonces

$$\begin{aligned} a + e \equiv a \pmod{m} &\Leftrightarrow e + a \equiv a \pmod{m} \\ &\Leftrightarrow e \equiv a - a \pmod{m} \\ &\Leftrightarrow e \equiv 0 \pmod{m} \end{aligned}$$

Luego, la clase $[e] = [0]$ Ó $e = 0$ es el neutro de la suma.

Prueba de la propiedad d (Opuesto)

Sea $[a] \in \mathbb{Z}_m$. Entonces el opuesto de $[a]$ es $[a'] = [-a]$.

$$\begin{aligned} [a] + [a'] = [0] \quad &\Leftrightarrow \quad [a + a'] = [0] \\ &\Leftrightarrow \quad a + a' \equiv 0 \pmod{m} \\ &\Leftrightarrow \quad a' \equiv -a \pmod{m} \\ &\Leftrightarrow \quad [a'] = [-a] \end{aligned}$$

Prueba de la propiedad c **(producto)**

Sea $[a] \in \mathbb{Z}_m$ y $[e]$ el elemento neutro del producto. Entonces

$$[e] \cdot [a] = [e \cdot a] = [a].$$

Luego, $[e] = [1]$ ó $e = 1$. Por tanto, el elemento neutro del producto es la clase $[1]$.

Prueba de la propiedad d (Inverso)

Sea $[a] \in \mathbb{Z}_m$. Entonces $[a]$ tiene **Inverso**, si y sólo si, $MCD(a, m) = 1$.

Sea $[a']$ el inverso de $[a]$ en $\mathbb{Z}$. Entonces

$$\begin{aligned} [a'] \cdot [a] = [1] &\Leftrightarrow [a' \cdot a] = [1] \\ &\Leftrightarrow a'a \equiv 1 \pmod{m} \\ &\Leftrightarrow a'a = 1 + mq, \; q \in \mathbb{Z} \\ &\Leftrightarrow aa' - mq = 1 \end{aligned}$$

Esta última ecuación tiene solución, si y sólo si, $MCD(a, m) = 1$ (a y m primos entre si).

Como $0 \leq a \leq m - 1$, puesto que $[a] \in \mathbb{Z}_m$, se tiene que:

1. Si m es primo, entonce $MCD(a, m) = 1$ para todo $a \neq 0$. Luego, todo elemento de $\mathbb{Z}_m$ tiene inverso, excepto el cero.
2. Si m no es primo, entonces sólo tienen inverso, aquellos elementos que sean primo con m.

Podemos decir que todo elemento de $\mathbb{Z}_m$ tiene inverso, si y sólo si, m es primo.

Ejemplo

Hallar el inverso de 3 en $\mathbb{Z}_7$.

Solución

Sea x el inverso de 3 en $\mathbb{Z}_7$. Entonces $3x = 1$ en $\mathbb{Z}_7$. Luego, $3x \equiv 1 \pmod 7$ en $\mathbb{Z}$.

Por consiguiente, $7 \mid 3x - 1$ en $\mathbb{Z}$. De aquí se deduce que $\exists y \in \mathbb{Z} : 3x - 7y = 1$.

Ahora obtenemos la solución general de la ecuación diofántica anterior, aplicando el algoritmo de Euclides.

Tenemos que

$$MCD(3, -7) = 1.$$

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= (-2) \cdot 3 + (-1)(-7) \\ &= 3 \cdot (-2) + (-7)(-1). \end{aligned}$$

De aquí que

$$\begin{aligned} x &= -2 + \frac{(-7)}{1}k, \quad k \in \mathbb{Z} \\ &= -2 - 7k = 5 - 7k. \end{aligned}$$

Nota: el -2 es congruente con 5 en $\mathbb{Z}_7$.

Luego, $x = 5$ en $\mathbb{Z}_7$ es el inverso de 3 en $\mathbb{Z}_7$.

Ejemplo

Hallar el inverso de 7 en $\mathbb{Z}_{16}$.

Solución

Como 7 y 16 son primos entre si, el 7 tiene inverso en $\mathbb{Z}_{16}$.

$$\begin{aligned} x \text{ es el inverso de 7 en } \mathbb{Z}_{16} &\Leftrightarrow 7x = 1 \text{ en } \mathbb{Z}_{16} \\ &\Leftrightarrow 7x \equiv 1 \pmod{16} \text{ en } \mathbb{Z} \\ &\Leftrightarrow 16 \mid 7x - 1 \text{ en } \mathbb{Z} \\ &\Leftrightarrow \exists y \in \mathbb{Z} : 7x - 16y = 1 \text{ en } \mathbb{Z} \end{aligned}$$

Utilizamos el algoritmo de Euclides para obtener una solución general de la ecuación diofántica anterior.

Tenemos que

$$MCD(7, -16) = 1.$$

Algoritmo de Euclides

$$\begin{aligned} 16 &= 2 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Ahora

$$\begin{aligned} 1 &= 7-3\cdot 2 \text{ (despeje del resto 1)} \\ &= 7-3(16-2\cdot 7) \text{ (despeje y sust. del resto 2)} \\ &= 7\cdot 7-3\cdot 16 \\ &= 7\cdot 7+3\cdot(-16) \\ &= 7\cdot 7+(-16)\cdot 3 \end{aligned}$$

De aquí que

$$\begin{aligned} x &= 7+\frac{(-16)}{1}k, \quad k\in\mathbb{Z} \\ &= 16q+7, \quad q=-k, \quad q\in\mathbb{Z} \end{aligned}$$

Luego, $x = 7$ en $\mathbb{Z}_{16}$ es el inverso de 7 en $\mathbb{Z}_{16}$.

Ley de cancelación en $\mathbb{Z}$

Sean $a, b, c \in \mathbb{Z}$. Si $ca = cb$, con $c \neq 0$, entonces $a = b$

Ley de cancelación en $\mathbb{Z}_m$

En $\mathbb{Z}_m$, la ley de cancelación no siempre se cumple. Por ejemplo,

$$3 \cdot 5 = 3 \cdot 3 \text{ en } \mathbb{Z}_6.$$

Sin embargo,

$$5 \neq 3.$$

Divisores de cero

Sea A un conjunto y sean $a, b \in A$. Decimos que a y b son **Divisores de cero**, si se verifica que:

$$a \cdot b = 0, \text{ siendo } a \neq 0 \wedge b \neq 0.$$

En $\mathbb{Z}$ no hay divisores de cero, porque si $a \cdot b = 0$, se tiene que $a = 0$ ó $b = 0$.

En $\mathbb{Z}_m$ hay divisores de cero. Es decir, es posible encontrar a y b, tales que $a \cdot b = 0$, siendo $a \neq 0$ y $b \neq 0$. Por ejemplo, en $\mathbb{Z}_{12}$, se tiene que

$$3 \cdot 8 = 0, \text{ siendo } 3 \neq 0 \wedge 8 \neq 0.$$

Ejemplo

Resolver el sistema en $\mathbb{Z}_7$.

$$\begin{array}{lrcrcr} (1) & 3x & + & 2y & = & 3 \\ (2) & x & + & 4y & = & 5 \end{array}$$

Solución

Aplicando el método de reducción tradicional, se tiene:

Multiplicando la ecuación (2) por 4, tenemos el sistema

$$\begin{array}{rcrcr} 3x & + & 2y & = & 3 \\ 4x & + & 2y & = & 6 \end{array}$$

Sumando ambas ecuaciones, obtenemos

$$4y = 2 \Rightarrow 4 \cdot 2y = 2 \cdot 2 \Rightarrow y = 4.$$

Ahora sustituimos en cualquiera de las ecuaciones originales, digamos en la ecuación (1), para tener

$$3x + 1 = 3 \Rightarrow 3x + 7 = 3 + 6 = 2 \Rightarrow 3x = 2 \Rightarrow 3 \cdot 5x = 2 \cdot 5 \Rightarrow x = 3.$$

Cualquiera de los métodos tradicionales puede ser aplicado para resolver el sistema.

Ejemplo

Resolver la ecuación $x^2 + 5x + 1 = 0$ en $\mathbb{Z}_5$.

Solución

Recuerde la fórmula general para resolver una ecuación de segundo grado:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

$$\begin{aligned} x &= \frac{-5 \pm \sqrt{5^2 - 4(1)(1)}}{2(1)} = \frac{-5 \pm \sqrt{25 - 4}}{2} = \frac{-5 \pm \sqrt{21}}{2} \\ &= \frac{-5 \pm \sqrt{20 + 1}}{2} = \frac{-5 \pm \sqrt{0 + 1}}{2} = \frac{-5 \pm \sqrt{1}}{2} \\ &= \frac{-5 \pm 1}{2} \end{aligned}$$

Luego,

$$x_1 = \frac{-5+1}{2} = \frac{-4}{2} = \frac{1}{2} = \frac{3\cdot 1}{3\cdot 2} = \frac{3}{1} = 3 \quad \therefore x_1 = 3$$

$$x_2 = \frac{-5-1}{2} = \frac{-6}{2} = \frac{4}{2} = \frac{3\cdot 4}{3\cdot 2} = \frac{2}{1} = 2 \quad \therefore x_2 = 2$$

Nota: El 3 es el inverso de 2 en $\mathbb{Z}_5$.

Función φ de Euler

Definición

Sea $m \in \mathbb{Z}^+$. La función de $\varphi(m)$ de Euler se define como

$$\varphi(m) = \left|\{k \in \mathbb{Z}^+ \mid k \leq m, \ \ MCD(k, m) = 1\}\right|.$$

Es decir, $\varphi(m)$ es el número de enteros positivos menores o iguales a m que sean primos relativos con m.

Ejemplo

$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(8) = 4.$

Algunas propiedades

1. $\varphi(m) = m - 1$, si m es primo.
2. $\varphi(m^k) = (m-1)m^{k-1}$, si m es primo y $k \in \mathbb{Z}^+$.
3. Si m y n son primos entre si, entonces $\varphi(mn) = \varphi(m)\varphi(n)$ (φ es una función multiplicativa).

El valor de $\varphi(m)$ se puede calcular haciendo uso del teorema fundamental de la aritmética:

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

donde los p_i son números primos distintos. Entonces combinando las propiedades 2 y 3, se tiene

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_r^{k_r}) \\ &= (p_1-1)p_1^{k_1-1}\,(p_2-1)p_2^{k_2-1}\cdots(p_r-1)p_r^{k_r-1}\end{aligned}$$

Luego, con un poco de álgebra en la expresión anterior, se obtiene

$$\varphi(m) = m\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

Ejemplo

Calcular $\varphi(700)$.

Solución

Sabemos que $700 = 2^2 \cdot 5^2 \cdot 7$.

$$\begin{aligned}\varphi(700) &= 700\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 700\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right) \\ &= 240\end{aligned}$$

Teorema de Euler

Sea $a \in \mathbb{Z}, \quad a \not\equiv 0 \pmod{m}$. Si a y m son primos relativos ($MCD(a, m) = 1$), entonces

$$a^{\varphi(m)} = 1 \text{ en } \mathbb{Z}_m.$$

Recuerde que esto quiere decir:

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demostración

Se deja como investigación para el estudiante.

Teorema de Fermat (Pequeño teorema de Fermat)

Sea $a \in \mathbb{Z}$ $a \not\equiv 0 \pmod{m}$. Si a y m son primos relativos ($MCD(a, m) = 1$), con m primo, entonces

$$a^{m-1} = 1 \quad \text{ó} \quad a^m = a \text{ en } \mathbb{Z}_m.$$

Demostración

La demostración es sumamente sencilla, puesto que es un caso particular del teorema de Euler, ya que m es primo ($\varphi(m) = m - 1$).

■

Ejemplo

Encuentre el resto de dividir 23^{2587} entre 7.

Solución

Según la división de Euclides, existen $q, r \in \mathbb{Z}$, únicos, tales que

$$23^{2587} = 7q + r,\ 0 \leq r < 7$$

Entonces

$$23^{2587} = r \text{ en } \mathbb{Z}_7.$$

Como $MCD(23, 7) = 1$, se tiene que el 23 es invertible en $\mathbb{Z}_7$. Adicionalmente, el 7 es primo. Por tanto, se tiene que

$$23^6 = 1 \text{ en } \mathbb{Z}_7.$$

Por otro lado, tenemos que

$$2587 = 6 \cdot 431 + 1.$$

Entonces

$$23^{2587} = 23^{6 \cdot 431+1} = 23^{6 \cdot 431} \cdot 23 = (23^6)^{431} \cdot 23.$$

Como $23^6 = 1$ y $23 = 2$ en $\mathbb{Z}_7$, se tiene

$$(23^6)^{431} = 1 \text{ en } \mathbb{Z}_7.$$

Luego,

$$(23^6)^{431} \cdot 23 = 1 \cdot 2 = 2 \text{ en } \mathbb{Z}_7.$$

Por tanto, el resto buscado es 2 en $\mathbb{Z}_7$.

Ejemplo

Demostrar que el número $(27^4)^9 - (25^3)^6$ es divisible por 37.

Solución

Debemos probar que

$$(27^4)^9 - (25^3)^6 = 0 \text{ en } \mathbb{Z}_{37}.$$

Entonces

$$(27^4)^9 - (25^3)^6 = 27^{36} - 5^{36}.$$

Sabemos que el 37 es primo. El 5 y 27 son primos relativos con 37. Luego, el 5 y 27 son invertibles en $\mathbb{Z}_{37}$. Aplicando el teorema de Fermat, se tiene que

$$27^{36} = 1 \text{ en } \mathbb{Z}_{37}.$$

$$5^{36} = 1 \text{ en } \mathbb{Z}_{37}.$$

Por tanto,

$$(27^4)^9 - (25^3)^6 = 27^{36} - 5^{36} = 0 \text{ en } \mathbb{Z}_{37}.$$

Luego, la cantidad $(27^4)^9 - (25^3)^6$ es divisible por 37.

Ejercicios

1. Determine los inversos de:
   a. 5 en $\mathbb{Z}_{11}$.
   b. 7 en $\mathbb{Z}_{17}$.
   c. 3 en $\mathbb{Z}_{12}$.
   d. 7 en $\mathbb{Z}_{18}$.
   e. 2 en $\mathbb{Z}_{13}$.
   f. 6 en $\mathbb{Z}_{15}$.
2. Construya las tablas de sumar y multiplicar en $\mathbb{Z}_5$ y $\mathbb{Z}_6$. Calcule opuesto e inverso de cada elemento según sea el caso.

3. Resuelva el siguiente sistema de ecuaciones en $\mathbb{Z}_7$.

$$\begin{array}{rcrcr} x & + & 2y & = & 4 \\ 4x & + & 3y & = & 4 \end{array}$$

4. Resueva la ecuación $x^2 + 3x + 4 = 0$ en $\mathbb{Z}_{11}$.
5. Si p es primo, demostrar que en $\mathbb{Z}_p$ se verifica la igualdad $(x + y)^p = x^p + y^p$.
6. Encuentre los divisores de cero en $\mathbb{Z}_5$.
7. Encuentre los elementos invertibles en $\mathbb{Z}_5$.

8. Resuelva el siguiente sistema de ecuaciones en $\mathbb{Z}_5$.

$$\begin{array}{rcrcl} 2x & + & 3y & = & 2 \\ 3x & + & 4y & = & 4 \end{array}$$

9. Encuentre $\varphi(48), \quad \varphi(104)$ y $\varphi(137)$.
10. Calcule el resto de dividir 3^{47} entre 23.
11. Demuestre que el resto de dividir 2^{340} entre 341 es 1.
12. Demuestre que si $MCD(a, 35) = 1$, entonces $a^{12} \equiv 1 \pmod{35}$.
13. Demuestre que $2^{70} + 3^{70}$ es divisible por 13.
14. Demuestre que $5^{38} \equiv 4 \pmod{11}$
15. Comprobar que 17 divide a $11^{104} + 1$.

Contenido

Definición

Sean $a, b, c \in \mathbb{Z}$. Una **Ecuación diofántica lineal** es toda ecuación de la forma

$$ax + by = c,$$

donde $x, y \in \mathbb{Z}$ son incógnitas.

Ejemplo

1. $4x + 9y = 7$
2. $8x - 12y = 20$

Teorema

Sean $a, b, c \in \mathbb{Z}$. La ecuación $ax + by = c$ tiene soluciones enteras, si y sólo si, $MCD(a, b) \mid c$.

Ejemplo

1. La ecuación $12x - 16y = 6$ no tiene solución, puesto que $MCD(12, 16) = 4 \not| 6$.
2. La ecuación $9x + 15y = 12$ tiene solución, puesto que $MCD(9, 15) = 3 \mid 12$.

Teorema (Bézout)

Sean $a, b \in \mathbb{Z}$, donde al menos uno de ellos es distinto de cero. Entonces existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$ax_0 + by_0 = MCD(a, b).$$

Cálculo de una solución particular de $ax + by = c$

1. Calcular $d = MCD(a, b) = r_n$ mediante el algoritmo de Euclides.
2. Verificar que $d \,|\, c$.

3. Calcular una solución particular u_0, v_0 de la ecuación $au + bv = MCD(a, b) = d$.

   Según el teorema de Bézout, existen $u_0, v_0 \in \mathbb{Z}$, tales que

$$au_0 + bv_0 = MCD(a, b) = r_n.$$

   Para calcular u_0 y v_0 procedemos despejando a $MCD(a, b) = r_n$ de la penúltima ecuación en el desarrollo del algoritmo de Euclides para obtener

$$r_n = r_{n-2} - r_{n-1}q_{n-1}. \quad (1)$$

Ahora despejamos a r_{n-1} de la ecuación antepenúltima y obtenemos la expresión resultante

$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}.$$

Sustituimos esta ecuación en la ecuación (1) para obtener

$$\begin{aligned} r_n &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1}. \\ &= r_{n-2}(1 + q_{n-1}q_{n-2}) - r_{n-3}q_{n-1} \end{aligned}$$

Si se continua el proceso, despejando los restos de las ecuaciones anteriores y sustituyéndolos en las ecuaciones

correspondientes, se llega a expresar a r_n como una combinación lineal de a y b, con lo que se consigue a u_0 y v_0. Es decir,

$$au_0 + bv_0 = r_n.$$

4. Cálculo de la solución particular $x_0, y_0 \in \mathbb{Z}$ de la ecuación $ax + by = c$.

   Como r_n divide a c, existe un $k \in \mathbb{Z}$, tal que

   $$c = kr_n.$$

   Luego,

   $$c = kr_n = a(ku_0) + b(kv_0).$$

De donde,

$$
\begin{aligned}
x_0 &= ku_0 = \frac{c}{r_n}u_0 \\
y_0 &= kv_0 = \frac{c}{r_n}v_0
\end{aligned}
$$

Solución general de la ecuación $ax + by = c$

Si la ecuación diofántica $ax + by = c$ tiene una solución particular $x_0, y_0 \in \mathbb{Z}$, entonces la solución general viene dada por

$$\begin{aligned} x &= x_0 + \frac{b}{MCD(a,b)}t \\ y &= y_0 - \frac{a}{MCD(a,b)}t, \end{aligned}$$

donde $t \in \mathbb{Z}$. Esto significa que la ecuación $ax + by = c$ tiene infinitas soluciones.

Ejemplo

Encuentre la solución general de la ecuación

$$12378x + 3054y = 3642.$$

Solución

Primero verifiquemos que la ecuación tiene solución, calculando el $d = MCD(12378, 3054)$ por el algoritmo de Euclides y comprobando que $d \mid 3642$.

$$\begin{aligned}
12378 &= 4 * 3054 + 162 \\
3054 &= 18 * 162 + 138 \\
162 &= 1 * 138 + 24 \\
138 &= 5 * 24 + 18 \\
24 &= 1 * 18 + 6 \\
18 &= 3 * 6 + 0
\end{aligned}$$

Luego, $d = MCD(12378, 3054) = 6$ (último resto distinto de cero).

El $d = MCD(12378, 3054) = 6$ divide a 3642. Es decir, $d \mid 3642$. Por tanto, la ecuación tiene solución.

Calculemos una solución particular de la ecuación

$$12378u + 3054v = d = 6.$$

Según el teorema de Bézout, existen $u_0, v_0 \in \mathbb{Z}$, tales que

$$12378u_0 + 3054v_0 = 6.$$

El procedimiento empieza despejando en el algoritmo de Euclides, el último resto distinto cero; luego el penúltimo, y así sucesivamente hasta llegar al primer resto, con lo que se obtiene una combinación lineal de los coeficientes de la ecuación. Los coeficientes que acompañan a los coeficientes de la ecuación en la combinación lineal

representan la solución particular u_0 y v_0 buscada. Recuerde que este es el mismo procedimiento explicado en el paso 3 anterior. Así

$$\begin{aligned} 6 &= 24 - 1 * 18 \\ &= 24 - 1 * (138 - 5 * 24) = 6 * 24 - 1 * 138 \\ &= 6 * (162 - 1 * 138) - 1 * 138 = 6 * 162 - 7 * 138 \\ &= 6 * 162 - 7 * (3054 - 18 * 162) = 132 * 162 - 7 * 3054 \\ &= 132 * (12378 - 4 * 3054) - 7 * 3054 = 132 * 12378 - 535 * 3054 \end{aligned}$$

Entonces $6 = 132 * 12378 - 535 * 3054$ y la solución particular buscada es

$$u_0 = 132, \ \ v_0 = -535.$$

Construyamos ahora una solución particular para la ecuación original.

$$3642 = 607 * 6 = (607 * 132) * 12378 - (607 * 535) * 3054.$$

La solución particular es :

$$x_0 = 607 * 132 = 80124, \quad y_0 = -607 * 535 = -324745.$$

Ahora encontramos la solución general:

$$\begin{aligned} x &= x_0 + \frac{b}{d}t = 80124 + \frac{3054}{6}t = 80124 + 509t \\ y &= y_0 - \frac{a}{d}t = -324745 - \frac{12378}{6}t = -324745 - 2063t, \end{aligned}$$

donde $t \in \mathbb{Z}$.

Ejercicios

1. Encuentre la solución general de la ecuación diofántica $6x + 10y = 72$.
2. Encuentre la solución general de la ecuación diofántica $31x + 8y = 180$.
3. Encuentre la solución general de la ecuación diofántica $87x - 64y = 3$.
4. Encuentre la solución general de la ecuación diofántica $3x + 6y = 18$.
5. Encuentre la solución general de la ecuación diofántica $2x + 10y = 17$.

6. Encuentre la solución general de la ecuación diofántica $5x + 6y = 8$.
7. Una empresa compró ciertos artículos a RD$17 c/u y vendió algunos de ellos a RD$49 c/u. Si la cantidad comprada originalmente es mayor que 50 y menor que 100 y la empresa obtuvo una ganancia de RD$245. ¿Cuántos artículos faltan por vender?.
8. Encuentre la solución general de la ecuación diofántica $343x - 51y = 735$.
9. Encuentre la solución general de la ecuación diofántica $150x + 60y = 6000$.

10. Una mujer va a una tienda y compra 12 vestidos; unos blancos y otros negros, por US$1200. Si los vestidos blancos valen US$30 más que los negros y ha comprado el mínimo posible de estos últimos, ¿cuántos vestidos ha comprado de cada color?
11. Encuentre la solución general de la ecuación diofántica $100x + 525y = 75$.
12. Encuentre la solución general de la ecuación diofántica $550x + 66y = 88$.
13. Halle los valores de $c \in \mathbb{Z}^+$, con $10 < c < 20$ para los cuales no tiene solución la ecuación diofántica $84x + 990y = c$. Determinar la solución para los restantes valores de c.

14. Halle las soluciones enteras de la ecuación

$$\sqrt{(x+y)(x-y)+(2x+2y-3)y-2(x-7)} = x+y+3.$$

15. Una persona compra 40 mangos por un valor total de US$10. Los mangos son de 10 centavos de dólar, 40 centavos de dólar y 1.4 dólares. ¿Cuántos mangos ha comprado de cada clase?.

Contenido

Definición

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$. Una ecuación de la forma

$$a \,.\, x \equiv b \,(\bmod\; m), \tag{1}$$

se le llama **Ecuación lineal de congruencia.**

Definición

Decimos que $x_0 \in \mathbb{Z}$ es **Solución** de la ecuación (1), si y sólo si, $m \,|\, (ax_0 - b)$.

Nota: Si x_0 es solución de (1) y x_1 es otro entero tal que $x_1 \equiv x_0 \,(\bmod\; m)$, entonces x_1 será también solución de la ecuación. Si la ecuación (1) tiene solución, posee infinitas.

Nos interesan solamente las soluciones que no sean congruentes entre si. Es decir, las que están dentro de $\mathbb{Z}_m$.

La ecuación (1) puede ser expresada como una ecuación diofántica en las variables x y y, en la forma

$$a\,.\,x - m\,.\,y = b, \tag{2}$$

donde y es un entero que debe determinarse. Se supone que las soluciones de (2) son enteras.

Teorema

La ecuación lineal de congruencia

$$a\,.\,x \equiv b\,(\bmod\ m), \tag{3}$$

posee solución, si y sólo si, $d \mid b$, donde $d = MCD(a, m)$. Si x_0 es una solución particular de (3), entonces la solución general viene dada por

$$x \equiv x_0 \,(\text{mód } \frac{m}{d}). \tag{4}$$

Demostración

La ecuación (3) se puede expresar en la forma

$$a \,.\, x - m \,.\, y = b. \tag{5}$$

y ésta es diofántica. Por tanto, según teorema de las ecuaciones diofánticas, estas tienen solución, si y sólo si, $d \mid b$, donde $d = MCD(a, m)$.

Aplicando la solución general de estas ecuaciones para x, se tiene

$$x = x_0 + \frac{m}{d}t, \;\; t = 0, 1, 2, \ldots, d-1.$$

El hecho de que el parámetro t tome sólo esos valores, se debe a que únicamente nos interesan las soluciones incongruentes entre si.

El número de soluciones incongruentes viene dado por $d = MCD(a, m)$.

Ejemplo

Resolver la ecuación lineal de congruencia

$$30x \equiv 15 \pmod{21}$$

Solución

Verifiquemos que la ecuación tiene solución, calculando $d = MCD(30, 21) = 3$. como 3 divide a 15, la ecuación tiene solución. Hay exactamente $d = 3$ soluciones en $\mathbb{Z}_{21}$.

Esta ecuación puede ser escrita como

$$30x - 21y = 15.$$

Nos interesa obtener una solución particular de esta ecuación y para ello, aplicamos el algoritmo de Euclides y el teorema de Bézout a la ecuación $30u - 21v = 3$:

Algoritmo de Euclides

$$\begin{aligned} 30 &= 1 \cdot 21 + 9 \\ 21 &= 2 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Teorema de Bézout

$$\begin{aligned} 3 &= 21 - 2 \cdot 9 \\ &= 21 - 2(30 - 1 \cdot 21) \\ &= 3 \cdot 21 - 2 \cdot 30 \\ &= -2 \cdot 30 + 3 \cdot 21 \\ &= -2 \cdot 30 - (-3)(21) \end{aligned}$$

La solución particular buscada es $u_0 = -2, \quad v_0 = -3$.

Ahora multiplicamos la ecuación por 5 y se obtiene

$$15 = (-10)(30) - (-15)(21).$$

De aquí que

$$x_0 = -10 = 11 \pmod{21}.$$

Aplicando la fórmula para x, tenemos

$$\begin{aligned} x_1 &= x_0 + \frac{(21)}{3}t = -10 + (7)(1) = -3 = 18 \,(\text{mód } 21) \\ x_2 &= x_0 + \frac{(21)}{3}t = -10 + (7)(2) = 4 \,(\text{mód } 21) \end{aligned}$$

Es decir, las soluciones son: 4, 11, 18.

Otra forma

Observemos que la ecuación se puede escribir como

$$3 \cdot 10x \equiv 3 \cdot 5 \pmod{21}.$$

Si aplicamos un resultado previo, la ecuación se transforma en

$10x \equiv 5 \pmod{7}$ y esta se puede simplificar como $3x \equiv 5 \pmod{7}$.

Como $MCD(3, 7) = 1$, se tiene que 3 es invertible en $\mathbb{Z}_7$ y por tanto, tiene inverso que es 5.

Luego, multiplicando por 5, se tiene

$$x \equiv 25 \pmod{7}, \quad \text{de donde} \quad x \equiv 4 \pmod{7}.$$

Recordemos que la formula para encontrar las soluciones es

$$x = x_0 + \frac{m}{d}t, \; t = 0, 1, 2, \cdots, d-1,$$

donde $x_0 = 4$ es la solución particular.

Es importante observar que la ecuación

$$3x \equiv 5 \pmod{7}$$

sólo tiene una solución. Sin embargo, necesitamos las soluciones de la ecuación original, que son tres (3).

Así que las soluciones son: $4, 4+7, 4+14$.

Ejemplo

Resolver la ecuación

$$51x \equiv 27 \pmod{123}.$$

Solución

Calculemos $d = MCD(51, 123) = 3$. Luego, la ecuación tiene solución y tiene 3 soluciones en $\mathbb{Z}_{123}$.

Tomemos la ecuación

$$51x - 123y = 27.$$

Apliquemos el algoritmo de Euclides y el teorema de Bézout a la ecuación

$$51u - 123v = 3.$$

para obtener una solución particular.

Algoritmo de Euclides

$$\begin{aligned} 123 &= 2 \cdot 51 + 21 \\ 51 &= 2 \cdot 21 + 9 \\ 21 &= 2 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Teorema de Bézout

$$\begin{aligned} 3 &= 21 - 2 \cdot 9 = 21 - 2(51 - 2 \cdot 21) \\ &= 5 \cdot 21 - 2 \cdot 51 \\ &= 5(123 - 2 \cdot 251) - 2 \cdot 51 \\ &= 5 \cdot 123 - 12 \cdot 51 \\ &= -12 \cdot 51 - (-5) \cdot 123 \end{aligned}$$

Entonces la solución particular buscada es $u_0 = -12, \quad v_0 = -5$.
Ahora multiplicamos por 9.

$$9 \cdot 3 = (-12 \cdot 9) \cdot 51 - (-5 \cdot 9) \cdot 123.$$

O sea que

$$27 = (-108)51 - (-45)123.$$

De donde una solución particular es

$$x_0 = -108 = 15 \pmod{123}.$$

Aplicando la fórmula para x se obtienen las demás soluciones:

$$\begin{aligned} x_1 &= x_0 + \frac{123}{3}t = -108 + 41(1) = -67 = 56 \pmod{123} \\ x_2 &= x_0 + \frac{123}{3}t = -108 + 41(2) = -26 = 97 \pmod{123} \end{aligned}$$

Teorema chino del resto

Si $m_1, m_2, \cdots, m_k$ son enteros positivos primos entre si dos a dos, entonces el sistema de ecuaciones

$$\begin{array}{ccl} x & = & a_1 \text{ en } \mathbb{Z}_{m_1} \\ x & = & a_2 \text{ en } \mathbb{Z}_{m_2} \\ x & = & a_3 \text{ en } \mathbb{Z}_{m_3} \\ . & \cdots & \cdots\cdots\cdots\cdots \\ x & = & a_k \text{ en } \mathbb{Z}_{m_k} \end{array}$$

tiene solución única

$$x = \sum_{i=1}^{k} a_i b_i y_i,$$

en $\mathbb{Z}_{m_1 \cdot m_2 \cdot m_3 \cdots m_k}$, donde los a_i son los valores dados en las ecuaciones; los b_i son los productos de los $m_j,\ j \neq i$ y los y_i son los inversos de los b_i en $\mathbb{Z}_{m_i}$.

Demostración

La demostración se deja como investigación para el estudiante.

Ejemplo

Hallar el menor número entero positivo que dividido por 3 da como resto 2; dividido por 5 da como resto 3 y dividido por 7 da resto 2.

Solución

Sea x el número que se busca. El sistema de ecuaciones que genera el problema es:

$$\begin{aligned} x &= 2 \text{ en } \mathbb{Z}_3 \\ x &= 3 \text{ en } \mathbb{Z}_5 \\ x &= 2 \text{ en } \mathbb{Z}_7 \end{aligned}$$

Los números 3, 5 y 7 son primos entre si, dos a dos. Aplicando el teorema chino del resto, se tiene que la solución en $\mathbb{Z}_{3 \cdot 5 \cdot 7} = \mathbb{Z}_{105}$ viene dada por

$$\begin{aligned} x &= 2 \cdot 5 \cdot 7 \cdot y_1 + 3 \cdot 3 \cdot 7 \cdot y_2 + 2 \cdot 3 \cdot 5 \cdot y_3 \\ &= 2 \cdot 35 y_1 + 3 \cdot 21 y_2 + 2 \cdot 15 y_3, \end{aligned}$$

donde los y_1, y_2, y_3 son los inversos de 35, 21 y 15 en $\mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$, respectivamente.

El inverso de 35 en $\mathbb{Z}_3$ es 2. Luego, $y_1 = 2$. Observemos que $35 = 2$ en $\mathbb{Z}_3$.

El inverso de 21 en $\mathbb{Z}_5$ es 1. Luego, $y_2 = 1$. Observemos que $21 = 1$ en $\mathbb{Z}_5$.

El inverso de 15 en $\mathbb{Z}_7$ es 1. Luego, $y_3 = 1$. Observemos que $15 = 1$ en $\mathbb{Z}_7$.

Por tanto,

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \text{ en } \mathbb{Z}_{105}.$$

Luego,

$$x = 23 \text{ en } \mathbb{Z}_{105}.$$

x es el menor entero positivo que satisface las condiciones del problema.

Los teoremas de Euler-Fermat ofrecen una fórmula explícita para resolver la congruencia

$$ax \equiv b \pmod{m},$$

cuando $MCD(a, m) = 1$. Esta fórmula es

$$x = ba^{\varphi(m)-1}.$$

Ejemplo

Resolver la congruencia $17x \equiv 9 \pmod{41}$.

Solución

Como $MCD(17, 41) = 1$, se tiene que $x = 9 \cdot 17^{39}$. Ahora debemos calcular a $17^{39} \pmod{41}$.

Convertimos el 39 como sumas de potencias de 2 y tenemos

$$39 = 2^0 + 2^1 + 2^2 + 2^5.$$

Luego,

$$\begin{aligned} 17^1 &= 17 \pmod{41} \\ 17^2 &= 289 = 2 \pmod{41} \\ 17^4 &= (17^2)^2 = 2^2 = 4 \pmod{41} \\ 17^8 &= (17^4)^2 = 4^2 = 16 \pmod{41} \\ 17^{16} &= (17^8)^2 = 16^2 = 10 \pmod{41} \\ 17^{32} &= (17^{16})^2 = 10^2 = 18 \pmod{41} \end{aligned}$$

Entonces

$$17^{39} = 17^{32} \cdot 17^4 \cdot 17^2 \cdot 17^1 = 18 \cdot 4 \cdot 2 \cdot 17 \equiv 29 \pmod{41}.$$

Luego,

$$x = 9 \cdot 29 \equiv 15 \pmod{41}.$$

1. Resuelva las ecuaciones

a.	$5x + 2 \equiv 5 \pmod{7}$	**b**.	$8x \equiv 12 \pmod{28}$
c.	$5x \equiv 7 \pmod{15}$	**d**.	$3x + 4 \equiv 5 \pmod{6}$
e.	$5x \equiv 1 \pmod{11}$	**f**.	$66x \equiv 42 \pmod{168}$
g.	$12x \equiv 9 \pmod{27}$	**h**.	$4x \equiv 3 \pmod{7}$
i.	$15x \equiv 18 \pmod{30}$		

2. Sabiendo que $MCD(a, 561) = 1$, justifique las afirmaciones siguientes:

   El número a verifica que

   a. 1) $a^2 \equiv 1 \pmod{3}$, 2) $a^{10} \equiv 1 \pmod{11}$, 3) $a^{16} \equiv 1 \pmod{17}$

   b. 1) $a^{560} \equiv 1 \pmod{2}$, 5) $a^{560} \equiv 1 \pmod{11}$, 3) $a^{560} \equiv 1 \pmod{17}$

3. Resuelva el sistema

$$\begin{aligned} x &= 32 \text{ en } \mathbb{Z}_{71} \\ x &= 84 \text{ en } \mathbb{Z}_{101} \end{aligned}$$

4. Resuelva el sistema

$$\begin{aligned} x &= 1 \text{ en } \mathbb{Z}_{3} \\ x &= 2 \text{ en } \mathbb{Z}_{5} \\ x &= 3 \text{ en } \mathbb{Z}_{7} \end{aligned}$$

5. Resuelva el sistema

$$\begin{aligned} x &= 5 \text{ en } \mathbb{Z}_{11} \\ x &= 14 \text{ en } \mathbb{Z}_{29} \\ x &= 15 \text{ en } \mathbb{Z}_{31} \end{aligned}$$

6. Resuelva las ecuaciones siguientes en los conjuntos indicados:
   a. $5x = 8$ en $\mathbb{Z}_6$
   b. $15x = 6$ en $\mathbb{Z}_{21}$
   c. $3x = 27$ en $\mathbb{Z}_6$
   d. $3x = 8$ en $\mathbb{Z}_6$
   e. $12x = 45$ en $\mathbb{Z}_3$

7. Resuelva el sistema

$$\begin{aligned} x &= 2 \text{ en } \mathbb{Z}_5 \\ 2x &= 1 \text{ en } \mathbb{Z}_7 \\ 3x &= 4 \text{ en } \mathbb{Z}_{11} \end{aligned}$$

8. Resuelva el sistema

$$\begin{aligned} x &= 2 \text{ en } \mathbb{Z}_4 \\ x &= 1 \text{ en } \mathbb{Z}_6 \\ 3x &= 4 \text{ en } \mathbb{Z}_{11} \end{aligned}$$

9. Resuelva la ecuación $x^2 = -1$, en $\mathbb{Z}_7$

10. Resuelva las siguientes ecuaciones por la forma explícita, si satisfacen las condiciones:
    a. $5x = 8$ en $\mathbb{Z}_6$
    b. $15x = 6$ en $\mathbb{Z}_{23}$
    c. $3x = 27$ en $\mathbb{Z}_6$
    d. $3x = 8$ en $\mathbb{Z}_7$
    e. $12x = 45$ en $\mathbb{Z}_5$

Contenido

Sean A y B dos conjuntos cualesquiera. Una **Relación** R, de A en B, es cualquier subconjunto del producto cartesiano $A \times B$. Se escribe $R : A \to B$. Al conjunto A se le llama **Conjunto de partida** y al conjunto B se le llama **conjunto de llegada**.
Cuando decimos que $a \in A$ está relacionado con $b \in B$, mediante la relación R, escribimos $(a, b) \in R$ o $a\,R\,b$. Cuando decimos que a no está relacionado con b mediante la relación R, escribimos $a \not R\, b$.
Una relación R, en A, es una relación de A en A.

Ejemplo

Sean $A = \{a, b, c\}$ y $B = \{3, 4, 5\}$ dos conjuntos.

Una relación $R : A \to B$ es $R = \{(a, 4), (b, 3), (c, 4)\}$.

En este caso, decimos que

$$a\,R\,4,\quad b\,R\,3,\quad c\,R\,4$$

o que

$$(a,4)\in R,\quad (b,3)\in R,\quad (c,4)\in R.$$

De la misma forma decimos que

$$a\,\not R\,3,\quad a\,\not R\,5.$$

Se llama **Dominio** de una relación $R : A \to B$, al subconjunto de A, cuyos elementos se relacionan con algún elemento de B. Se representa por D_R. Se llama **Codominio o Rango** de una relación

$R : A \to B$ al subconjunto de B, cuyos elementos están relacionados con algún elemento de A. Se escribe C_R.

En el caso del ejemplo, el dominio de R es

$$D_R = \{a, b, c\} \text{ y el codominio es } C_R = \{4, 3\}.$$

Ejemplo

Sea $A = \{a, b, c\}$ un conjunto.

Podemos definir una relación $R : A \to A$ como $R = \{(a, c), (b, b), (b, a)\}$.

Aquí

$$D_R = \{a, b\}, \quad C_R = \{c, b, a\}.$$

Definición

Se llama **Conjunto solución** de una relación $R : A \to B$ al conjunto de pares ordenados que definen la relación. Por ejemplo, el conjunto solución de la relación del ejemplo anterior es R.

Definición

La relación **Idéntica o diagonal** en A se define como una relación $\Delta : A \to A$ tal que

$$\Delta = \{(a, a)|a \in A\}$$

Cuando tenemos una relación $R : A \to A$, decimos que R es una relación sobre A.

Sean A y B dos conjuntos finitos, donde $|A| = m$ y $|B| = n$. Entonces $|A \times B| = |A||B| = mn$. Así que el número de relaciones de A a B que se pueden construir viene dado por

$$2^{mn},$$

que es el número de subconjuntos de $A \times B$.

Definición

Un **enunciado formal** es una cualidad o característica común que satisfacen las componentes de los pares ordenados que definen una relación. Por ejemplo, sea $A = \{2, 3, 4, 6\}$ y sea $R : A \to A$, cuyo

enunciado formal es " x divide a y". Entonces la relación viene definida por

$$R = \{(2,2),(2,4),(2,6),(3,3),(3,6),(4,4),(6,6)\}.$$

Ejemplo

Sea $A = \{1,2,3\}$ y sea $R : A \to A$, cuyo enunciado formal es " $2x + y \leq 5$ ". Entonces la relación viene definida por

$$R = \{(1,1),(1,2),(1,3),(2,1)\}.$$

Ejemplo

Sea A el conjunto de personas que viven en una ciudad. Podemos definir relaciones mediante enunciados formales como:

Relaciones

“x es el padre de y”
“x es hermano de y”
“x es padrino de y”

Definición

Consideremos los conjuntos $A = \{a_1, a_2, a_3, \dots, a_m\}$ y $B = \{b_1, b_2, b_3, \dots, b_n\}$. Sea R una relación de A en B. La **representación matricial de** R viene dada por la matriz booleana de m filas y n columnas:

$$M_R = \begin{pmatrix} r_{1,1} & \cdots & \cdots & \cdots & r_{1,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & r_{i,j} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ r_{m,1} & \cdots & \cdots & \cdots & r_{m,n} \end{pmatrix},$$

donde

$$r_{i,j} = \begin{cases} 1, & \text{si } (a_i, b_j) \in R \\ 0, & \text{si } (a_i, b_j) \notin R \end{cases}$$

Ejemplo

Sean los conjuntos $A = \{2, 3, 5\}$ y $B = \{4, 6, 9, 10\}$. Sea R la relación de A en B, cuyo enunciado formal es "x divide a y". El conjunto solución viene dado por

$$R = \{(2, 4), (2, 6), (2, 10), (3, 6), (3, 9), (5, 10)\}.$$

La representación matricial de R viene dada por

$$M_R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Definición

Consideremos los conjuntos $A = \{a_1, a_2, a_3, \ldots, a_m\}$ y $B = \{b_1, b_2, b_3, \ldots, b_n\}$. Sean R y S dos relaciónes binarias de A en B, cuyas representaciones matriciales son:

$$M_R = (r_{i,j}) \text{ y } M_S = (s_{i,j}).$$

Si consideramos las tablas de verdad de las operaciones lógicas en términos booleanos, se producen las siguientes propiedades:

a. $M_{R\cup S} = M_R \vee M_S = M_R \oplus M_S = r_{ij} + s_{ij}$.
b. $M_{R\cap S} = M_R \wedge M_S = r_{ij} \,.\, s_{ij}$.
c. $M_{R^c} = \neg M_R$.
d. $M_{R-S} = M_R \wedge \neg M_S$.

e. $(R \subseteq S) \leftrightarrow (M_R \to M_S) \leftrightarrow \forall i, j : r_{i,j} \to s_{i,j}$ o
$(R \subseteq S) \leftrightarrow (M_R \leq M_S) \leftrightarrow r_{ij} \leq s_{ij}, \forall i, j$.

f. $R = S \leftrightarrow (M_R \to M_S) \wedge (M_S \to M_R) \leftrightarrow M_R = M_S$.

Definición

Sean A y B dos conjuntos cualesquiera.

La relación **Inversa** de una relación $R : A \to B$, es la relación $R^{-1} : B \to A$, cuyos pares ordenados se obtienen intercambiando las componentes de los pares ordenados de la relación R. Es decir,

$$R^{-1} = \{(b, a) \in B \times A | (a, b) \in R\}.$$

Ejemplo

Sean $A = \{3, 4, 5\}$ y $B = \{a, b, c\}$ dos conjuntos.

Consideremos la relación $R : A \to B$, definida por $R = \{(3, c), (5, a), (5, b)\}$. Entonces la relación inversa $R^{-1} : B \to A$ viene dada por

$$R^{-1} = \{(c, 3), (a, 5), (b, 5)\}.$$

Definición

La representación matricial de la inversa, R^{-1}, de una relación $R \subseteq A \times B$, se define como la transpuesta de la representación matricial de la relación R. Es decir,

$$M_{R^{-1}} = M_R^t.$$

Ejemplo

La representación matricial de la relación R del ejemplo previo es

$$M_R = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad M_{R^{-1}} = M_R^t = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Definición

Sean $A = (a_{ij})$ y $B = (b_{ij})$ dos matrices boolenas de orden $m \times k$ y $k \times n$, respectivamente. El **producto booleano** de A y B se define como la matriz $C = A \odot B$, de orden $m \times n$, donde

$$c_{ij} = \sum_{l=1}^{k} a_{il} \cdot b_{lj} = a_{i1} \cdot b_{1j} \oplus a_{i2} \cdot b_{2j} \oplus a_{i3} \cdot b_{3j} \oplus \cdots \oplus a_{ik} \cdot b_{kj}.$$

Definición

Sean A, B y C conjuntos no vacíos. Sean $R \subseteq A \times B$ y $S \subseteq B \times C$ dos relaciones. La **Composición** de R y S, representada por $R \circ S$ es la relación $T \subseteq A \times C$, definida por

$$T = R \circ S = \{(a, c) \in A \times C \,|\, \exists b \in B \wedge (a, b) \in R \wedge (b, c) \in S\}$$

La representación matricial de $R \circ S$ viene dada por

$$M_{R \circ S} = M_R \odot M_S.$$

Ejemplo

Sean $A = \{a, b, c\}$, $B = \{3, 4, 5\}$, $C = \{1, 2\}$. Sea $R \subseteq A \times B$, tal que $R = \{(a, 4), (a, 5), (c, 3)\}$ y $S \subseteq B \times C$, tal que $S = \{(4, 1), (3, 1), (3, 2)\}$. Entonces

$$R \circ S = \{(a, 1), (c, 1), (c, 2)\}.$$

Ahora bien,

$$M_R = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad M_S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$M_{R \circ S} = M_R \odot M_S = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \odot \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}$$

Definición

Sea R una relación sobre un conjunto dado A. Las potencias de R se definen en forma recursiva como:

a. $R^1 = R$

b. $R^{n+1} = R \circ R^n$

En términos de la representación matricial, se tiene

a. $M_R^1 = M_R$

b. $M_R^{n+1} = M_R \odot M_R^n$

Ejemplo

Sea $A = \{a, b, c, d\}$ y $R : A \to A$ tal que

$$R = \{(a, b), (a, d), (c, a), (d, d), (b, c)\}.$$

Entonces

$R^2 = R \circ R = \{(a, c), (a, d), (c, b), (c, d), (d, d), (b, a)\}$
$R^3 = R \circ R^2 = \{(a, a), (a, d), (c, c), (c, d), (d, d), (b, b), (b, d)\}$

Definición

Una relación R sobre un conjunto A es **Reflexiva** si para todo $a \in A$, se tiene que $(a, a) \in R$.

Ejemplo

Sea $A = \{1, 2, 3\}$ y $R : A \to A$, cuyo enunciado formal es "x divide a y". Es evidente que

$$(1, 1) \in R, \quad (2, 2) \in R, \quad (3, 3) \in R.$$

R es reflexiva $\Leftrightarrow \Delta \subseteq R \Leftrightarrow M_\Delta \leq M_R$. Es decir, si y sólo si, tiene unos (1_s) en todos los elementos de la diagonal principal. M_Δ es la representación matricial de la relación diagonal.

Ejemplo

Sea A el conjunto de todas las personas que viven en una ciudad. Sea R una relación sobre A, cuyo enunciado formal es "x tiene el mismo nombre que y".

Solución

Es claro que x tiene el mismo nombre que x para todo $x \in A$. Por tanto, es reflexiva.

Definición

Una relación R sobre un conjunto A es **Irreflexiva o antireflexiva** si para todo $a \in A$, se tiene que $(a, a) \notin R$.

Ejemplo

Sea $A = \{1, 2, 3\}$ y $R : A \to A$, cuyo enunciado formal es "$x < y$".

$$R = \{(1,2),(1,3),(2,3)\}.$$

Es evidente que

$$(1,1) \notin R, \quad (2,2) \notin R, \quad (3,3) \notin R.$$

R es irreflexiva $\Leftrightarrow R \cap \Delta = \emptyset \Leftrightarrow M_R \wedge M_\Delta = M_0$. Es decir, si y sólo si, no tiene unos (1_s) en todos los elementos de la diagonal principal. M_0 es la matriz nula (todos sus elementos cero).

Si una relación no es reflexiva, se dice que es no reflexiva. Las relaciones irreflexivas son casos particulares de relaciones no reflexivas. Las relaciones no reflexivas y no irreflexivas se caracterizan de la siguiente manera:

No reflexivas $\Leftrightarrow \exists a \in A \ni (a, a) \notin R$.

No irreflexivas $\Leftrightarrow \exists a \in A \ni (a, a) \in R$

Definición

Una relación R sobre un conjunto A es **Simétrica** si cuando $(a, b) \in R$, se tiene que $(b, a) \in R$.

Ejemplo

Sea $A = \{1, 2, 3\}$ y $R : A \to A$, tal que $R = \{(1, 1), (2, 3), (3, 2), (3, 3)\}$. Es claro que R es simétrica.

R es simétrica $\Leftrightarrow (R = R^{-1}) \Leftrightarrow M_R = M_R^t$.

Ejemplo

Sea $A = \{x \mid x$ es una persona que vive en Santo Domingo$\}$ y $R : A \to A$, cuyo enunciado formal es "x tiene el mismo nombre que y". Es evidente que si a tiene el mismo nombre que b; b tiene el mismo nombre que a. De modo que si $(a, b) \in R$ se tiene que $(b, a) \in R$ y R es simétrica.

Definición

Una relación R sobre un conjunto A es **Antisimétrica** si cuando $(a, b) \in R$ y $(b, a) \in R$, se tiene que $a = b$.

Ejemplo

Sea $A = \{1, 2, 3\}$ y $R : A \to A$, tal que $R = \{(1, 1), (1, 2), (2, 3), (3, 3)\}$. Es claro que R es antisimétrica.

R es antisimétrica $\Leftrightarrow (R \cap R^{-1} \subseteq \Delta) \Leftrightarrow (M_R \wedge M_R^t \leq M_\Delta)$, donde M_Δ es la representación matricial de la relación Δ.

Definición

Una relación R sobre un conjunto A es **Asimétrica** si cuando $(a, b) \in R$, se tiene que $(b, a) \notin R$ y $\forall a \in A$, se tiene que $(a, a) \notin R$.

Ejemplo

Sea $A = \{1, 2, 3\}$ y $R : A \to A$, tal que $R = \{(1, 2), (1, 3), (2, 3)\}$. Es claro que R es asimétrica.

R es asimétrica $\Leftrightarrow (R \cap R^{-1} = R_\emptyset) \Leftrightarrow M_R \wedge M_R^t = M_0$, donde M_0 es la matriz, cuyos elementos son todos cero y $R_\emptyset$ es la relación vacía.

Definición

Una relación R sobre un conjunto A es **Transitiva** si cuando $(a, b) \in R$ y $(b, c) \in R$, se tiene que $(a, c) \in R$.

Ejemplo

Sea $A = \{1, 2, 3\}$ y $R : A \to A$, tal que $R = \{(1, 1), (2, 3), (3, 2), (2, 2), (3, 3)\}$. Es claro que R es transitiva.

R es transitiva $\Leftrightarrow R \circ R \subseteq R \Leftrightarrow M_R \odot M_R \leq M_R$.

Ejemplo

Sea $A = \{x \,|\, x$ es una persona que vive en Santo Domingo$\}$ y $R : A \to A$, cuyo enunciado formal es “x tiene el mismo nombre que

y". Es evidente que si a tiene el mismo nombre que b y b tiene el mismo nombre que c, se tiene que a tiene el mismo nombre que c. De modo que R es transitiva.

Cierres o clausuras

Cierre reflexivo

Sea R una relación sobre un conjunto A. EL **Cierre reflexivo de** R es la relación reflexiva más pequeña que contiene a R como subconjunto y se define como

$$CR(R) = R \cup \Delta$$

o

$$M_{CR(R)} = M_R \oplus M_\Delta.$$

Ejemplo

Sea $A = \{1, 2, 3, 4\}$ y R una relación sobre A, tal que $R = \{(1, 2), (3, 4), (1, 1)\}$. El cierre reflexivo de R viene dado por

$$CR(R) = \{(1, 2), (3, 4), (1, 1), (2, 2), (3, 3), (4, 4)\}.$$

Es decir, se agrega la cantidad mínima de elementos que la haga reflexiva.

Cierre simétrico

Sea R una relación sobre un conjunto A. El **Cierre simétrico de** R es la relación simétrica más pequeña que contiene a R como subconjunto y se define como

$$CS(R) = R \cup R^{-1}$$

o

$$M_{CS(R)} = M_R \oplus M_R^t.$$

Ejemplo

Sea $A = \{1, 2, 3, 4\}$ y R una relación sobre A, tal que $R = \{(1, 2), (3, 4), (1, 1)\}$. El cierre simétrico de R viene dado por

$$CS(R) = \{(1, 2), (3, 4), (1, 1), (2, 1), (4, 3)\}.$$

Es decir, se agrega la cantidad mínima de elementos que la haga simétrica.

Cierre transitivo

Sea R una relación sobre un conjunto A. EL **Cierre transitivo de** R es la relación transitiva más pequeña que contiene a R como subconjunto y se define como

$$CT(R) = R \cup R^2 \cup R^3 \cup \cdots \cup R^k$$

o

$$M_{CT(R)} = M_R \oplus M_R^2 \oplus M_R^3 \oplus \cdots \oplus M_R^k.$$

Ejemplo

Sea $A = \{a, b, c, d\}$ y R una relación sobre A, tal que $R = \{(a, b), (b, c), (c, d)\}$. Calculamos

$$R^2 = R \circ R = \{(a, c), (b, d)\}, \quad R^3 = R \circ R^2 = \{(a, d)\}, \quad R^4 = R \circ R^3 = \emptyset.$$

Luego, el cierre transitivo de R viene dado por

$$\begin{aligned} CT(R) &= R \cup R^2 \cup R^3 \\ &= \{(a, b), (b, c), (c, d), (a, c), (b, d), (a, d)\}. \end{aligned}$$

Es decir, se agrega la cantidad mínima de elementos que la haga transitiva.

Ejercicios

1. Sea $A = \{2, 3, 4, 5\}$ y R una relación en A, cuyo enunciado formal es "x es primo relativo con y".
   a. Escriba a R como un conjunto de pares ordenados.
   b. Haga el diagrama de coordenadas de R.
   c. Determine a R^{-1}.
2. Sea $A = \mathbb{N}$ y R una relación en A, cuyo enunciado formal es "$x + 2y = 8$".
   a. Escriba a R como un conjunto de pares ordenados.
   b. Determine a R^{-1}.
3. Sea $A = \{1, 2, 3, 4, 5\}$ y R una relación en A, cuyo enunciado formal es "x es primo relativo con y". Encuentre los cierres reflexivo, simétrico y transitivo.

Contenido

Definición

Una relación R sobre un conjunto A es una **Relación de equivalencia** sobre A si satisface las propiedades siguientes:

a. Reflexiva

b. Simétrica

c. Transitiva

Ejemplo

Sea $A = \{x \,|\, x$ es una persona que vive en Santo Domingo$\}$ y $R : A \to A$, cuyo enunciado formal es "x tiene el mismo nombre que y". Es claro que esta relación es reflexiva, simétrica y transitiva, por tanto, es de equivalencia.

Ejemplo

Sea $A = \mathbb{R}$ y $R : A \to A$, cuyo enunciado formal es "$x = y$". Es evidente que esta relación es reflexiva, simétrica y transitiva, por tanto, es de equivalencia.

Ejemplo

Sea $A = \{a, b, c, d\}$ y $R : A \to A$, tal que
$R = \{(a, a), (a, b), (b, a), (b, b), (c, d), (d, c), (c, c), (d, d)\}$.

Es fácil verificar que esta relación es reflexiva, simétrica y transitiva, por tanto, es de equivalencia.

Ejemplo

Sea $A = \emptyset$ y $R : A \to A$, tal que $R = \emptyset$.

Es fácil verificar que esta relación es reflexiva, simétrica y transitiva, por tanto, es de equivalencia. Sin embargo, esta relación no es de equivalencia sobre un conjunto no vacío, ya que no es reflexiva.

Ejemplo

La congruencia módulo n es una relación de equivalencia.

Solución

Debemos comprobar que se cumplen las tres propiedades: reflexiva, simétrica y transitiva.

Reflexiva

$$a \equiv a \pmod{n}, \quad \text{puesto que } \; a - a = 0 \, . \, n.$$

Simétrica

Si $a \equiv b \pmod{n}$, entonces $a - b = k \, . \, n, \;\; k \in \mathbb{Z}$. Pero $b - a = -(a - b) = -k \, . \, n, \;\; -k \in \mathbb{Z}$. Por tanto, $b \equiv a \pmod{n}$.

Transitiva

Si $a \equiv b \pmod{n}$, entonces $a - b = k_1 \,.\, n, \quad k_1 \in \mathbb{Z}$ y
si $b \equiv c \pmod{n}$, entonces $b - c = k_2 \,.\, n, \quad k_2 \in \mathbb{Z}$.
Ahora bien, sumando miembro a miembro, se tiene que
$a - c = (k_1 + k_2) \,.\, n, \quad (k_1 + k_2) \in \mathbb{Z}$. Por tanto, $a \equiv c \pmod{n}$.

Definición

Dado un conjunto A y una relación de equivalencia R sobre el conjunto A. Se llama **Clase de equivalencia** de un elemento $a \in A$ al subconjunto de A definido por

$$[a] = \{x \in A \,|\, (x, a) \in R\}.$$

Ejemplo

Sea $A = \{1, 2, 3\}$ y $R : A \to A$, una relación de equivalencia definida por $R = \{(1, 1), (2, 3), (3, 2), (2, 2), (3, 3)\}$. Entonces

$[1] = \{1\}$
$[2] = \{3, 2\}$

$[3] = \{2, 3\}$

Ejemplo

Sea $A = \mathbb{Z}$ y $R : A \to A$, una relación de equivalencia definida por $R = \{(x, y) \mid x = y\}$. Entonces para $a \in A$ se tiene que $[a] = \{x \in A \mid x = a\} = \{a\}$

Ejemplo

Sea $A = \mathbb{Z}$ y $R : A \to A$, una relación de equivalencia definida por $R = \{(x, y) \mid x = y \vee x = -y\}$. Entonces para $a \in A$ se tiene que $[a] = \{x \in A \mid x = a \vee x = -a\} = \{a, -a\}$

Ejemplo

Sea $A = \mathbb{Z}$ y $R : A \to A$, una relación de equivalencia definida por $R = \{(x, y) \mid x \equiv y \pmod 7\}$. Entonces para $a \in A$ se tiene que $[a] = \{x \in A \mid a \equiv x \pmod 7\} = \{x \in A \mid \exists k \in \mathbb{Z},\, a - x = 7k\}$.

Algunos casos de muestra son:

$$[0] = \{\dots, -21, -14, -7, 0, 7, 14, 21, 28, \dots\} = \{7k \mid k \in \mathbb{Z}\}$$
$$[1] = \{\dots, -20, -13, -6, 1, 8, 15, 22, 29, \dots\} = \{7k + 1 \mid k \in \mathbb{Z}\}$$
$$[2] = \{\dots, -19, -12, -5, 2, 9, 16, 23, 30, \dots\} = \{7k + 2 \mid k \in \mathbb{Z}\}$$

Recordemos que este ejemplo fue tratado anteriormente.

Definición

Al conjunto de todas las clases de equivalencia con respecto a la relación de equivalencia R sobre un conjunto A se le llama **Conjunto cociente** de A por R y se representa generalmente por A/R. Es decir,

$$A/R = \{[x] \,|\, x \in A\}.$$

Ejemplo

Sea $A = \{1, 2, 3, 4, 5\}$ y la relación de equivalencia
$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1), (2,4)(4,2)\}$. Entonces
$[1] = \{1,3\}, \quad [2] = \{2,4\}, \quad [3] = \{1,3\}$
$[4] = \{2,4\}, \quad [5] = \{5\}$

Así que $A/R = \{[1], [2], [3], [4], [5]\} = \{[1], [2], [5]\} = \{\{1,3\}, \{2,4\}, \{5\}\}$
Ejemplo

Sea $A = \mathbb{Z}$ y la relación de equivalencia $R = \{(x, y) \mid x \equiv y \pmod 7\}$. EL conjunto cociente viene dado por

$$A/R = \{[0], [1], [2], [3], [4], [5], [6]\}.$$

Ejercicios

1. Sea $A = \{1, 2, 3, 4\}$
   a. Escriba un ejemplo de una relación que sea reflexiva, simétrica y no transitiva.
   b. Escriba un ejemplo de una relación que sea simétrica y transitiva pero no reflexiva.
   c. Escriba un ejemplo de una relación que sea reflexiva y antisimétrica pero no transitiva.
   d. Escriba un ejemplo de una relación que sea reflexiva, simétrica y transitiva.

   e. Escriba un ejemplo de una relación que sea reflexiva, antisimétrica y transitiva.
2. Usando el conjunto A del punto 1, encuentre el cierre reflexivo de la relación $R = \{(1, 2), (2, 3), (2, 4), (3, 1)\}$.

3. Usando el conjunto A del punto 1, encuentre el cierre transitivo de la relación $R = \{(1,1),(1,3),(2,1),(2,3),(2,4),(3,2),(3,4),(4,1)\}$.
4. ¿Cuáles de las relaciones del conjunto $A = \{a,b,c,d\}$ son de equivalencia y contienen los pares (a,b) y (b,d)?.
5. Sean los conjuntos $A = \{1,2,3,4\}$ y $B = \{1,3,5\}$. Sea $R \subseteq A \times B$, cuyo enunciado formal es "$x < y$". Encuentre el conjunto solución.
6. Sea $A = \mathbb{N}$ y $R \subseteq \mathbb{N} \times \mathbb{N}$, definida por

$$R = \{(1,5),(4,5),(1,4),(4,6),(3,7),(7,6)\}.$$

Determine D_R, C_R y R^{-1}.

7. Sea $A = \{a, b, c, d\}$ y R una relación sobre A, cuya representación matricial es

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Determine los conjuntos
$E_b = \{x \in A | (x, b) \in R\}, \quad E_d = \{x \in A | (d, x) \in R\}.$

8. Sea $A = \{1, 2, 3, 4, 5\}$ y $R \subseteq A \times A$, cuya representación matricial es

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Determine D_R, C_R y R^{-1}.

9. Sea $A = \{1, 2, 3, 4\}$ y $R \subseteq A \times A$, definida por

$$R = \{(1,1),(2,2),(1,3),(3,1)(3,3),(3,4)\}.$$

¿Cuáles propiedades cumple y cuáles no?.

10. Sea $A = \{a, b, c, d\}$, $R \subseteq A \times A$ y $S \subseteq A \times A$, definidas por $R = \{(b,b),(b,c),(a,d),(d,b)\}$ y $S = \{(a,b),(c,a),(d,a)\}$.
    a. Encuentre la representación de cada relación.
    b. Encuentre $(R \circ S)^{-1}$, $S \circ R$, $(R \cup S)^{-1}$.
    c. D_R y $C_{S^{-1}}$.

11. Sea $A = \mathbb{N}$ y $R \subseteq A \times A$, cuyo enunciado formal es “$2x + y = 16$”. ¿Cuáles propiedades cumple y cuáles no?.

12. Sea $A = \{1, 2, 3, 4\}$ y sean las relaciones sobre A, $R_1 = \{(1, 1), (1, 2)\}$, $R_2 = \{(1, 1), (2, 3), (4, 1)\}$, $R_3 = \{(1, 3), (2, 4)\}$, $R_4 = \{(1, 1), (2, 2), (3, 3)\}$, $R_5 = A \times A$, $R_6 = \emptyset$. Determine cuáles son reflexivas, simétricas y transitivas.

13. Sea $A = \{1, 2, 3, 4, 5, 6\}$ y $R \subseteq A \times A$, definida por $R = \{(1, 1), (2, 1), (1, 2), (2, 2), (3, 3), (4, 4), (4, 5), (5, 4), (5, 5), (6, 6)\}$. ¿Es R un relación de equivalencia?. Si es así, cuál es su conjunto cociente?.

14. Sean $A_1 = \{1, 2\}$, $A_2 = \{2, 3, 4\}$, $A_3 = \{5\}$. Sea $A = A_1 \cup A_2 \cup A_3$. Sea $R \subseteq A \times A$, cuyo enunciado formal es “x y y están en el mismo conjunto $A_i, i = 1, 2, 3$”. ¿Es R una relación de equivalencia?.

Ejercicios

15. Sea $A = \mathbb{R}^2$ y $R \subseteq A \times A$, cuyo enunciado formal "$(x_1, y_1)R(x_2, y_2) \leftrightarrow x_1 = x_2$". Verifique que R es una relación de equivalencia.
16. Sea $A = \{1, 2, 3, 4, 5, 6, 7\}$ y $R \subseteq A \times A$, cuyo enunciado formal es "$x - y$ es múltiplo de 3". Demuestre que R es una relación de equivalencia y calcule las clases de equivalencia generadas por R.

17. Sea $A = \mathbb{Z}^2$ y $R \subseteq A \times A$, cuyo enunciado formal "$(x_1, y_1)R(x_2, y_2) \leftrightarrow x_1 y_2 = y_1 x_2$". Verifique que R es una relación de equivalencia. encuentre $[(4, 8)]$.

18. Sea $A = \mathbb{N}^2$ y $R \subseteq A \times A$, cuyo enunciado formal "$(x_1, y_1)R(x_2, y_2) \leftrightarrow x_1 + y_2 = y_1 + x_2$". Verifique que R es una relación de equivalencia. Encuentre $[(3, 7)]$.

19. Sea $A_1 = \{1, 2, 3, 4, 5\}$, $A = A_1 \times A_1$ y $R \subseteq A \times A$, cuyo enunciado formal "$(x_1, y_1)R(x_2, y_2) \leftrightarrow x_1 + y_1 = x_2 + y_2$". Verifique que R es una relación de equivalencia. Encuentre $[(1, 3)]$, $[(2, 4)]$ y $[(1, 1)]$. Encuentre la partición de A generada por R.

Definición

Sea A un conjunto. Una **Partición** de A es una familia $\{A_i\}_{i \in I}$ de subconjuntos no vacíos de A que satisface las siguientes propiedades:

a. $A = \bigcup\limits_{i \in I} A_i$

b. $A_i \cap A_j = \emptyset, \quad i \neq j$

Ejemplo

Sea $A = \{1, 2, 3, 4, 5, 6, 7\}$. Las siguientes colecciones son particiones de A.

a. $A_1 = \{1, 3, 4\}, \quad A_2 = \{2, 7\}, \quad A_3 = \{5, 6\}$

b. $A_1 = \{3, 4, 7\}, \quad A_2 = \{1, 2, 5\}, \quad A_3 = \{6\}$

c. $A_k = \{k\}, \quad k = 1, 2, \ldots, 7$

Ejemplo

Sea $A = \mathbb{Z}$. Las siguientes colecciones son particiones de A.

a. $A_1 = \{x \,|\, x = 2k, \quad k \in \mathbb{Z}\}, \qquad A_2 = \{x \,|\, x = 2k + 1, \quad k \in \mathbb{Z}\}$

b. $A'_k = \{3k, 3k + 1, 3k + 2\}, \quad k \in \mathbb{N}$

$A''_k = \{-3k, -3k + 1, -3k + 2\}, \quad k \in \mathbb{Z}^+$

Teorema

Sea R una relación de equivalencia sobre un conjunto A y sean $x, y \in A$. Entonces se verifican las siguientes propiedades:

a. $x \in [x]$

b. $(x, y) \in R,$ si y sólo si $[x] = [y]$

c. $[x] = [y]$ ó $[x] \cap [y] = \emptyset$

Demostración

a. $x \in A$ y como R es reflexiva, se tiene que $(x, x) \in R$ y por tanto, $x \in [x]$

b. Debemos probar los casos siguientes

   1. Si $(x, y) \in R$, entonces $[x] = [y]$.
   2. Si $[x] = [y]$, entonces $(x, y) \in R$.

Caso 1. Sea $(x,y) \in R$. Debemos probar que $[x] \subseteq [y]$ y $[y] \subseteq [x]$.

Sea $a \in [x]$. Entonces $(x,a) \in R$. $(a,x) \in R$. $(a,x) \in R \wedge (x,y) \in R$. $(a,y) \in R$. Luego, $a \in [y]$ y $[x] \subseteq [y]$.

Sea $a \in [y]$. Entonces $(y,a) \in R$. $(x,y) \in R \wedge (y,a) \in R$. $(x,a) \in R$. Luego, $a \in [x]$ y $[y] \subseteq [x]$. Por tanto,

$$[x] = [y].$$

Caso 2. Sea $[x] = [y]$. Como $x \in [x]$, se tiene que $x \in [y]$ y por tanto, $(x,y) \in R$.

c. Supongamos que $[x] \cap [y] \neq \emptyset$. Entonces existe $a \in [x] \cap [y]$. $a \in [x] \wedge a \in [y]$. $(x, a) \in R \wedge (y, a) \in R$. $(x, a) \in R \wedge (a, y) \in R$. $(x, y) \in R$. Luego, $[x] = [y]$, según el caso b.
De esta forma podemos concluir que

$$[x] = [y] \vee [x] \cap [y] = \emptyset.$$

Teorema

Si R es una relación de equivalencia sobre el conjunto A, entonces R genera una Partición de A.

Demostración

Debemos probar que

$$A/R = \{[x] \mid x \in A\}$$

es una partición de A. Es decir, probar que este conjunto satisface las dos condiciones de una partición.

Por definición, se tiene que $[x] \neq \emptyset$ y $[x] \subseteq A$.

Sabemos que $\forall\, x, y \in A, \quad [x] = [y] \vee [x] \cap [y] = \emptyset$.

Necesitamos probar que $A = \bigcup_{x \in A} [x]$ y para ello debemos demostrar que

1. $A \subseteq \bigcup_{x \in A} [x]$
2. $\bigcup_{x \in A} [x] \subseteq A$

Prueba de 1.

Sea $x \in A$. Entonces $x \in [x]$ y por tanto, $x \in \bigcup_{x \in A} [x]$. Luego,

$$A \subseteq \bigcup_{x \in A} [x]$$

Prueba de 2.

Sea $x \in \bigcup_{x \in A} [x]$. Entonces $\exists y \in A \ni x \in [y]$. Como $[y] \subseteq A$, se tiene que $x \in A$. Luego,

$$\bigcup_{x \in A} [x] \subseteq A \qquad \blacksquare$$

Teorema

Toda partición del conjunto A, define una relación de equivalencia sobre A.

Demostración

Sea $\{A_i \,|\, i \in I\}$ una partición del conjunto A. Consideremos la relación $R = \{(x, y) \,|\, \exists i \in I, x, y \in A_i\}$.
Debemos probar que R satisface las propiedades de una relación de equivalencia.

- Reflexiva

Si $x \in A$, entonces $\exists i \in I$, tal que $x \in A_i$, puesto que $A = \bigcup_{i \in I} A_i$.
Entonces $\exists i \in I$, tal que $x \in A_i \wedge x \in A_i$ y por tanto, $(x, x) \in R$.

- Simétrica

Sea $(x, y) \in R$. Entonces $\exists i \in I$, tal que $x \in A_i \wedge y \in A_i = y \in A_i \wedge x \in A_i$. Entonces $(y, x) \in R$. Por tanto, si $(x, y) \in R$, se tiene que $(y, x) \in R$.

- Transitiva

Sea $(x, y) \in R \wedge (y, z) \in R$. Entonces $\exists i \in I$, tal que $x \in A_i \wedge y \in A_i$ y $\exists j \in I$, tal que $y \in A_j \wedge z \in A_j$. Entonces $\exists i, j \in I$, tal que $x \in A_i, y \in A_i \cap A_j, z \in A_j$. Como $A_i \cap A_j \neq \emptyset$, se sigue que $A_i = Aj$. Entonces $\exists i \in I$, tal que, $x \in A_i, z \in A_i$ y $(x, z) \in R$. Por tanto, si $(x, y) \in R \wedge (y, z) \in R$, se tiene que $(x, z) \in R$. ■

1. Sea $A = \{a, b, c, d\}$. Considere las relaciones en A.
$R_1 = \{(a, a), (a, b),\quad R_2 = \{(a, c), (b, d)\},\quad R_3 = A \times A$
$R_4 = \{(a, a), (b, c), (d, a)\},\quad R_5 = \{(a, a), (b, b), (c, c)\},\quad R_6 = \emptyset$
Determine cuáles son reflexivas, simétricas, transitivas.

2. Sea A el conjunto de todas las líneas en un plano y R una relación en A, cuyo enunciado formal es "x es perpendicular a y". Determine, si R es una relación de equivalencia.

3. Sea A el conjunto de todos los triángulos de un plano y $R : A \to A$, cuyo enunciado es "x es semejante a y". Determine si es una relación de equivalencia.

4. Sea A el conjunto de todos los círculos de un plano y $R : A \to A$, cuyo enunciado es "x tiene igual radio que y". Determine si es una relación de equivalencia.
5. Sea $A = \mathbb{N}$ y $R : A \to A$, cuyo enunciado es "x es el cuadrado de y". Determine si es una relación de equivalencia.

6. Sea A el conjunto de todos los polígonos de un plano y $R : A \to A$, cuyo enunciado es "x tiene el mismo número de vértices que y". Determine si es una relación de equivalencia.
7. Sea $A = \mathbb{R}$ y $R : A \to A$, cuyo enunciado es "$x \leq y$". Determine si es una relación de equivalencia.

8. Sea A una colección de conjuntos y $R : A \to A$, cuyo enunciado es "$x \subseteq y$". Determine si es una relación de equivalencia.
9. Sea A el conjunto de todas las líneas de un plano y $R : A \to A$, cuyo enunciado es "$x \,||\, y$". Determine si es una relación de equivalencia.

10. Sea $A = \{a, b, c, d\}$. Determine las propiedades de las siguientes relaciones:
a. $R_1 = \{(a, b), (d, c), (b, b), (b, a), (c, a)\}$
b. $R_2 = \{(b, b), (b, c), (c, b)\}$
c. $R_3 = \{(a, c)\}$
11. Sea A el conjunto de todas las líneas de un plano y $R : A \to A$. Demuestre que
a. R es reflexiva, si y sólo si, $R_I \subseteq R$
b. R es simétrica, si y sólo si, $R = R^{-1}$

12. Sea $A = \mathbb{N}$ y R una relación sobre $A \times A$, definida por

$(a, b) \cong (c, d)$, si y sólo si $ad = bc$.

Demuestre que R es una relación de equivalencia.

13. Sea $A = \{1, 2, 3, 4, 5, 6, 7\}$. ¿Cuáles de las siguientes familias son particiones de A.

a. $A_1 = \{1, 3, 5\}, \quad A_2 = \{2\}, \quad A_3 = \{4, 7\}$

b. $B_1 = \{1, 5, 7\}, \quad B_2 = \{3, 4\}, \quad B_3 = \{2, 5, 6\}$

c. $C_1 = \{1, 2, 5, 7\}, \quad C_2 = \{3\}, \quad C_3 = \{4, 6\}$

d. $D_1 = \{1, 2, 3, 4, 5, 6, 7\}$

14. Sea $A = \{a, b, c, d\}$. Encuentre todas las particiones de A

15. Sea $A = \mathbb{N}$ y R una relación en $A \times A$, definida por

$$(a, b) \cong (c, d), \text{ si y sólo si, } a + d = b + c.$$

a. Demuestre que R es una relación de equivalencia
b. Encuentre $[(2, 5)]$.

16. Sean R y S relaciones de equivalencia en un conjunto A. Demuestre que $R \cap S$ es una relación de equivalencia en A.
17. Sean R y S relaciones reflexiva y simétrica en un conjunto A. Demuestre que $R \cup S$ es una relación reflexiva y simétrica en A.

18. Presente un ejemplo de relaciones transitivas R y S para las cuales $R \cup S$ no es transitiva.

19. Sean A y B subconjuntos de U. Pruebe que $A \cap B$, $A \cap B'$, $A' \cap B$ y $A' \cap B'$ forman una partición de U.

Contenido

Definición

Sea A un conjunto y R una relación binaria sobre A. Decimos que R es una **relación de orden** , si satisface las siguientes propiedades:

a. Reflexiva
b. Antisimétrica
c. Transitiva

Un conjunto sobre el cual se haya definido una relación de orden R, se llama **ordenado** respecto a dicha relación y se representa por (A, R) o de modo más general, $(A, \preceq)$.

Ejemplo

Sea $A = \{1, 2, 3\}$. Consideremos la relación de inclusión sobre el conjunto potencia de A, $P(A)$. Es claro que esta relación, es una relación de orden por que satisface las propiedades reflexiva, antisimétrica y transitiva.

Podemos ordenar el conjunto $P(A)$ como

$$\{\} \subseteq \{1\} \subseteq \{1, 2\} \subseteq \{1, 2, 3\}$$

o de la siguiente forma

$$\{\} \subseteq \{3\} \subseteq \{1,3\} \subseteq \{1,2,3\}$$

Si hay elementos en el conjunto entre los cuales no se puede establecer la relación, decimos que el conjunto está **parcialmente ordenado**, por ejemplo

$$\{2\} \not\subseteq \{3\} \text{ ni } \{3\} \not\subseteq \{2\}.$$

Es evidente que la relación $<$ no es de orden en $\mathbb{Z}^+$, puesto que no es reflexiva.

Definición

Sea A un conjunto y $\preceq$ una relación de orden sobre A. Los elementos x y y en A son **comparables** mediante la relación $\preceq$, si $x \preceq y$ o $y \preceq x$. En caso contario, se dice que no son comparables.

Definición

Sea A un conjunto y $\preceq$ una relación de orden sobre A. Decimos que $\preceq$ es una **relación de orden parcial**, si hay elementos en A que no son comparables. Es decir, si $\exists x, y \in A \ni (x \not\preceq y \wedge y \not\preceq x)$.

Ejemplo

La relación de inclusión es una relación de orden parcial, ya que hay por lo menos dos elementos en $P(A)$ que no son comparables.

Ejemplo

Sea $A = \mathbb{Z}^+$ y $\preceq$ la relación de "$x|y$" (x divide a y). Es claro que $\preceq$ es una relación de orden parcial.

Definición

Sea A un conjunto y $\preceq$ una relación de orden sobre A. Decimos que $\preceq$ es una **relación de orden total** si todos los elementos de A son comparables. Es decir, si

$$\forall x, y \in A : x \preceq y \ \vee \ y \preceq x.$$

En este caso, se dice que A está totalmente ordenado. Por ejemplo, las relaciones $\leq$ y $\geq$ son relaciones de orden total en los conjuntos $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{R}$.

Definición

Sea A un conjunto y $\preceq$ una relación de orden sobre A. Decimos que $\preceq$ es una **relación de orden densa** si

$$\forall x, y \in A : x \preceq y,\; x \neq y$$

existe otro elemento $z \in A$ tal que

$$x \preceq z,\; x \neq z \;\text{ y }\; z \preceq y,\; z \neq y.$$

Por ejemplo, si $A = \mathbb{Q}$, la relación $\leq$ hace del conjunto $\mathbb{Q}$ un conjunto densamente ordenado.

Sea $A = \mathbb{Z}$ y la relación de orden $\leq$. Es evidente que este conjunto no es densamente ordenado, porque entre dos elementos consecutivos no hay otro elemento.

Más sobre relaciones de orden

Sea $\preceq$ una relación de orden sobre un conjunto A. Entonces si

$x \preceq y$, se dice que x es anterior a y o que x precede a y.

Si $x \preceq y$, $x \neq y$, se escribe $x \prec y$ y se dice que x precede estrictamente a y o que x es estrictamente anterior a y.

$x \succeq y$, se dice que x es posterior a y o que x sucede a y.

Si $x \succeq y$, $x \neq y$, se escribe $x \succ y$ y se dice que x sucede estrictamente a y o que x es estrictamente posterior a y.

Ejemplo

Probar que la relación "$\leq$" de $\mathbb{Z}$ es de orden.

Prueba

Primeramente, definamos que

$$a \leq b \;\Leftrightarrow\; b - a \geq 0 \;\Leftrightarrow\; b - a \in \mathbb{N} \;\Leftrightarrow\; \exists k \in \mathbb{N} \ni b - a = k$$

Reflexiva

Sea $a \in \mathbb{Z}$. Entonces $a = a,\; a - a = 0,\; 0 \in \mathbb{N}$. Luego, $a \leq a$ y la relación es reflexiva.

Antisimétrica

Sean $a, b \in \mathbb{Z}$. Entonces

$$a \leq b \;\Leftrightarrow\; \exists k_1 \in \mathbb{N} \ni b - a = k_1$$

y

$$b \leq a \;\Leftrightarrow\; \exists k_2 \in \mathbb{N} \ni a - b = k_2.$$

Entonces $k_1 = -k_2$. Pero como $k_1, k_2 \in \mathbb{N}$, necesariamente $k_1 = k_2 = 0$.
Por lo tanto, $b - a = 0$ y $a - b = 0$. Luego,

$$a = b$$

y la relación es antisimétrica.

Transitividad

Sean $a, b, c \in \mathbb{Z}$. Entonces

$$a \leq b \;\Leftrightarrow\; \exists k_1 \in \mathbb{N} \ni b - a = k_1$$

y

$$b \leq c \;\Leftrightarrow\; \exists k_2 \in \mathbb{N} \ni c - b = k_2.$$

Entonces

$$b - a + c - b = c - a = k_1 + k_2 = k \in \mathbb{N}.$$

Luego, $a \leq c$ y la relación es transitiva.

Definiciones

Sean X y $A \neq \emptyset$ dos conjuntos tales que $A \subseteq X$. Sea $\preceq$ una relación de orden sobre X.

1. Un elemento $\alpha \in X$, tal que $\alpha \preceq x$, para todo $x \in A$, se le llama **Cota inferior** de A. Se dice que A está **Acotado inferiormente**.

Más sobre relaciones de orden

2. Un elemento $\beta \in X$, tal que $x \preceq \beta$, para todo $x \in A$, se le llama **Cota superior** de A. Se dice que A está **Acotado superiormente**.
3. El conjunto A es **Acotado**, si lo es superior e inferiormente.
4. Un elemento $a \in A$, tal que $\forall x \in A: \; x \preceq a \Rightarrow a = x$, se le llama **Elemento minimal** de A. Es decir, si no existe $x \in A$ tal que $x \prec a$.
5. Un elemento $a \in A$, tal que $\forall x \in A: \; a \preceq x \Rightarrow a = x$, se le llama **Elemento maximal** de A. Es decir, si no existe $x \in A$ tal que $a \prec x$.
6. Un elemento $a \in A$, tal que $a \preceq x$, para todo $x \in A$, se le llama **Elemento mínimo** de A.

7. Un elemento $a \in A$, tal que $x \preceq a$, para todo $x \in A$, se le llama **Elemento máximo** de A.
8. Al elemento máximo del conjunto de todas las cotas inferiores de A se le llama **Ínfimo** de A. Se escribe $\text{ínf } A$.
9. Al elemento mínimo del conjunto de todas las cotas superiores de A se le llama **Supremo** de A. Se escribe $\sup A$.

Teorema

Si $(A, \preceq)$ es un conjunto ordenado y finito, entonces tiene al menos un elemento maximal y un elemento minimal.

Demostración

Supongamos que el conjunto $(A, \preceq)$ es ordenado con n elementos.

Sea $a \in A$.

Si a no es minimal, entonces

$$\exists m \leq n \ni a_m \in A \wedge a_m \preceq a.$$

Si a_m no es minimal, entonces

$$\exists a_{m-1} \in A \ni a_{m-1} \preceq a_m \preceq a.$$

Puesto que A es finito, este proceso debe terminar en algún momento y llegaremos a tener

$$a_1 \preceq a_2 \preceq \cdots \preceq a_m \preceq \cdots \preceq a_n \preceq a.$$

Luego, no es posible tener un elemento $b \in A$ tal que $b \prec a_1$. Por tanto, a_1 es un elemento minimal.

Para probar lo del elemento maximal, se procede de manera similar.

Teorema (Unicidad)

Si el conjunto ordenado y finito $(A, \preceq)$ tiene mínimo (máximo), este es único.

Demostración

Supongamos que A tiene dos mínimos, m_1 y m_2. Como m_1 es mínimo, se tiene que $m_1 \preceq m_2$ y como m_2 es mínimo, se tiene que $m_2 \preceq m_1$. Luego, por la propiedad antisimétrica, se concluye que

$$m_1 = m_2.$$

Y el mínimo es único.

Para el máximo se procede de manera similar.

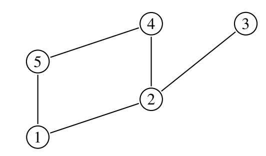
Diagramas de Hasse de un conjunto finito ordenado $(X, \preceq)$

Es una representación gráfica del mismo en la que cada elemento se representa por un punto del plano, con las siguientes características:

1. Como la relación es reflexiva, Se eliminan todos los bucles.
2. Si $a \preceq b$, se dibuja a por debajo de b y se une a con b por medio de un segmento. En ocasiones, el segmento tiene flecha hacia b, en cuyo caso no es necesario que se dibuje a por debajo de b.
3. Se suprimen los segmentos que corresponden a la propiedad transitiva. Es decir, si $a \preceq b \ \wedge \ b \preceq c$,se elimina el segmento $a \preceq c$.

Ejemplo

Considere el conjunto ordenado $X = \{1, 2, 3, 4, 5\}$, según el diagrama de Hasse siguiente. Sea $A = \{1, 2, 5\}$.



Encontrar cotas inferiores y superiores, elementos minimales y maximales, mínimos y máximos, ínfimos y supremos.

Solución

Más sobre relaciones de orden

1. El 4 es una cota superior y a la vez supremo.
2. El 2 y 5 son elementos maximales.
3. No tiene máximo.
4. El 1 es cota inferior, ínfimo, mínimo y es el único elemento minimal.

Ejemplo

Sean $X = \mathbb{Z}, \quad A = \{3, 4, 5, 6, 7, 8, 9, 10\}$. Sea $R : A \to A$ una relación de orden, tal que $x \preceq y \Leftrightarrow x \mid y$.

1. Encuentre los elementos minimales y maximales.
2. Halle los subconjuntos de A totalmente ordenados.

Solución

$$R = \{(3,3),(3,6),(3,9),(4,4),(4,8),(5,5),(5,10),(6,6),(7,7),(8,8),(9,9),(10,10)\}$$

1. El 3, 4, 5, 7 son elementos minimales y el 6, 7, 8, 9 y 10 son elementos maximales.
2. Subconjuntos totalmente ordenados.
   a. $\{x\}_{x\in A}$.
   b. $\{3,6\},\ \{3,9\},\ \{4,8\},\ \{5,10\}$.

Ejemplo

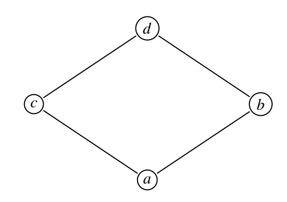
Sean $A = \{a, b, c, d\}$ y
$R = \{(a, a), (a, b), (b, b), (b, d), (a, c), (c, c), (c, d), (a, d), (d, d)\}$. Entonces

1. Compruebe que R es de orden.
2. Haga el diagrama de Hasse.
3. Analice si es orden total.
4. Determine si existen mínimo y máximo.

Solución

1. Es fácil comprobar que es de orden

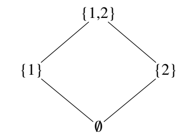
2. El diagrama de Hasse es :



3. No es de orden total porque $c \not\preceq b$ y $b \not\preceq c$.
4. a es el elemento mínimo y d es el elemento máximo.

Ejemplo

Sea $S = \{1, 2\}$ y $A = P(S)$. El diagrama de Hasse del conjunto parcialmente ordenado $(A, \subseteq)$ es



Definición

Decimos que un conjunto ordenado X está **Bien ordenado**, si todo subconjunto no vacío de X tiene un elemento mínimo.

Teorema

Todo conjunto bien ordenado está totalmente ordenado.

Definición

Una relación R sobre un conjunto A se dice que es de **Orden estricto**, si satisface las propiedades siguientes:

a. Asimétrica

b. Transitiva

Ejemplo

Probar que la relación "$<$" en $\mathbb{Z}$ es de orden estricto.

Prueba

Debemos empezar por dar la siguiente definición

$$a < b \;\Leftrightarrow\; b - a > 0 \;\Leftrightarrow\; b - a \in \mathbb{Z}^{+} \;\Leftrightarrow\; \exists k \in \mathbb{Z}^{+} \ni b - a = k$$

Asimétrica

Sean $a, b \in \mathbb{Z}$. Entonces

$$a < b \;\Leftrightarrow\; b - a > 0 \;\Leftrightarrow \exists k \in \mathbb{Z}^{+} \ni b - a = k.$$

Entonces

$$a - b = -k,\ a - b \notin \mathbb{Z}^+,\ a - b \neq k,\ \forall k \in \mathbb{Z}^+,\ b \nless a$$

y la relación es asimétrica.

Transitividad

Sean $a, b, c \in \mathbb{Z}$. Entonces

$$a < b \ \Leftrightarrow\ \exists k_1 \in \mathbb{Z}^+ \ni b - a = k_1$$

y

$$b < c \ \Leftrightarrow\ \exists k_2 \in \mathbb{Z}^+ \ni c - b = k_2.$$

Entonces

$$b - a + c - b = c - a = k_1 + k_2 = k \in \mathbb{Z}^+.$$

Luego, $a < c$ y la relación es transitiva.

Teorema

Si $(A, \preceq_1)$ y $(B, \preceq_2)$ son dos conjuntos parcialmente ordenados, entonces el conjunto $(A \times B, \preceq)$ también es parcialmente ordenado, con el orden definido por

$$(a_1, b_1) \preceq (a_2, b_2) \Leftrightarrow a_1 \preceq_1 a_2 \ \wedge \ b_1 \preceq_2 b_2.$$

Demostración

Reflexiva

Sea $(a, b) \in A \times B$. Entonces

$$\begin{aligned}(a,b) \in A \times B &\Leftrightarrow a \in A \wedge b \in B \\ &\Leftrightarrow a \preceq_1 a \wedge b \preceq_2 b \\ &\Leftrightarrow (a,b) \preceq (a,b)\end{aligned}$$

Luego,

$$\forall\, (a,b) \;:\; [(a,b) \in A \times B \Leftrightarrow (a,b) \preceq (a,b)].$$

Antisimétrica

Orden del producto

Sean $(a_1, b_1), (a_2, b_2) \in A \times B$. Entonces

$$\begin{cases} (a_1, b_1) \preceq (a_2, b_2) \\ \qquad\wedge \\ (a_2, b_2) \preceq (a_1, b_1) \end{cases} \Leftrightarrow \begin{cases} a_1 \preceq_1 a_2 \wedge b_1 \preceq_2 b_2 \\ \qquad\wedge \\ a_2 \preceq_1 a_1 \wedge b_2 \preceq_2 b_1 \end{cases}$$

$$\Leftrightarrow \begin{cases} a_1 \preceq_1 a_2 \wedge a_2 \preceq_1 a_1 & \text{en } A \\ \qquad\wedge \\ b_1 \preceq_2 b_2 \wedge b_2 \preceq_2 b_1 & \text{en } B \end{cases}$$

$\Rightarrow \quad a_1 = a_2 \wedge b_1 = b_2$ antisimetría de $\preceq_1$ y $\preceq_2$

$\Leftrightarrow \quad (a_1, b_1) = (a_2, b_2)$

Luego, $\forall\,(a_1,b_1),(a_2,b_2)\in A\times B:$

$[(a_1,b_1)\preceq(a_2,b_2)\wedge(a_2,b_2)\preceq(a_1,b_1)\Rightarrow(a_1,b_1)=(a_2,b_2)].$

Transitiva

Sean $(a_1,b_1),(a_2,b_2),(a_3,b_3)\in A\times B$. Entonces

$$\begin{cases}(a_1,b_1)\preceq(a_2,b_2)\\ \qquad\quad\wedge\\ (a_2,b_2)\preceq(a_3,b_3)\end{cases}\Leftrightarrow\begin{cases}a_1\preceq_1 a_2\ \wedge\ b_1\preceq_2 b_2\\ \qquad\quad\wedge\\ a_2\preceq_1 a_3\ \wedge\ b_2\preceq_2 b_3\end{cases}$$

$$\Leftrightarrow \quad \begin{cases} a_1 \preceq_1 a_2 \ \wedge \ a_2 \preceq_1 a_3 & \text{en } A \\ \qquad\qquad \wedge & \\ b_1 \preceq_2 b_2 \ \wedge \ b_2 \preceq_2 b_3 & \text{en } B \end{cases}$$

$$\Rightarrow \quad a_1 \preceq_1 a_3 \ \wedge \ b_1 \preceq_2 b_3 \ \text{ por transitividad de } \preceq_1 \text{ y } \preceq_2$$

$$\Leftrightarrow \quad (a_1, b_1) \preceq (a_3, b_3)$$

Luego,

$\forall\, (a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B :$

$[(a_1, b_1) \preceq (a_2, b_2) \ \wedge \ (a_2, b_2) \preceq (a_3, b_3) \Rightarrow (a_1, b_1) \preceq (a_3, b_3)]$.

Ejemplo

Consideremos el conjunto $\mathbb{Z}^+ \times \mathbb{Z}^+$. Definimos la relación

$$(a, b) \preceq (a', b') \Leftrightarrow a \,|\, a' \wedge b \leq b',$$

donde "$|$" es la operación de divisibilidad y "$\leq$" es el orden común. Probar que la relación $\preceq$ es de orden.

Solución

Reflexiva

Sea $(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. Entonces

$(a, b) \preceq (a, b)$ puesto que $a \mid a$ por ser "|" reflexiva y $b \leq b$ por ser "$\leq$" reflexiva. Es decir,

$$\forall (a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+, (a, b) \preceq (a, b) \text{ y por tanto, reflexiva.}$$

Antisimétrica

Sean $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. Entonces

$$\begin{cases}(a_1, b_1) \preceq (a_2, b_2) \\ \quad\quad\wedge \\ (a_2, b_2) \preceq (a_1, b_1)\end{cases} \Leftrightarrow \begin{cases}a_1 \mid a_2 \wedge b_1 \leq b_2 \\ \quad\quad\wedge \\ a_2 \mid a_1 \wedge b_2 \leq b_1\end{cases}$$

$$\Leftrightarrow \begin{cases}a_1 \mid a_2 \wedge a_2 \mid a_1 & \text{en } \mathbb{Z}^+ \\ \quad\quad\wedge \\ b_1 \leq b_2 \wedge b_2 \leq b_1 & \text{en } \mathbb{Z}^+\end{cases}$$

$$\Rightarrow \quad a_1 = a_2 \wedge b_1 = b_2 \quad \text{antisimetría de “}|\text{” y “}\leq\text{”}$$

$$\Leftrightarrow \quad (a_1, b_1) = (a_2, b_2)$$

Luego,

$\forall\, (a_1, b_1), (a_2, b_2) \in \mathbb{Z}^+ \times \mathbb{Z}^+ :$

$[(a_1, b_1) \preceq (a_2, b_2) \wedge (a_2, b_2) \preceq (a_1, b_1) \Rightarrow (a_1, b_1) = (a_2, b_2)].$

Transitiva

Sean $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. Entonces

$$\begin{cases} (a_1, b_1) \preceq (a_2, b_2) \\ \qquad \wedge \\ (a_2, b_2) \preceq (a_3, b_3) \end{cases} \Leftrightarrow \begin{cases} a_1 \,|\, a_2 \wedge b_1 \leq b_2 \\ \qquad \wedge \\ a_2 \,|\, a_3 \wedge b_2 \leq b_3 \end{cases}$$

$$\Leftrightarrow \begin{cases} a_1 \mid a_2 \wedge a_2 \mid a_3 & \text{en } \mathbb{Z}^+ \\ \qquad \wedge & \\ b_1 \leq b_2 \wedge b_2 \leq b_3 & \text{en } \mathbb{Z}^+ \end{cases}$$

$\Rightarrow \quad a_1 \mid a_3 \wedge b_1 \leq b_3$ por transitividad de "$|$" y " $\leq$ "

$\Leftrightarrow \quad (a_1, b_1) \preceq (a_3, b_3)$

Luego,

$\forall\, (a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{Z}^+ \times \mathbb{Z}^+$:

$[(a_1, b_1) \preceq (a_2, b_2) \wedge (a_2, b_2) \preceq (a_3, b_3) \Rightarrow (a_1, b_1) \preceq (a_3, b_3)]$.

Orden lexicográfico

El orden lexicográfico es el orden utilizado en el diccionario y guías tefefónicas. Es muy útil en el procesamiento de cadenas. Aunque aquí lo vamos aplicar a dos conjuntos, el mismo puede ser generalizado a n conjuntos.

Teorema

Sean $(A, \preceq_1)$ y $(B, \preceq_2)$ dos conjuntos parcialmente ordenados. El **Orden lexicográfico** es una relación de orden, $\preceq$, en el producto $A \times B$, definida como:

$$(a_1, b_1) \preceq (a_2, b_2) \Leftrightarrow a_1 \prec_1 a_2 \vee (a_1 = a_2 \wedge b_1 \preceq_2 b_2),$$

donde $a_1 \prec_1 a_2,$ si $a_1 \preceq_1 a_2 \wedge a_1 \neq a_2$.

Demostración

Reflexiva

Sea $(a, b) \in A \times B$. Entonces

$(a, b) \preceq (a, b) \Leftrightarrow a \prec_1 a \vee (a = a \wedge b \preceq_2 b) \Leftrightarrow (a = a \wedge b \preceq_2 b)$, por ser $\preceq_2$ reflexiva. Luego, $(a, b) \preceq (a, b)$, y por tanto, reflexiva.

Antisimétrica

Sean $(a_1, b_1), (a_2, b_2) \in A \times B$. Entonces

Orden lexicográfico

$$\left\{\begin{array}{c}(a_1, b_1) \preceq (a_2, b_2) \\ \wedge \\ (a_2, b_2) \preceq (a_1, b_1)\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}a_1 \prec_1 a_2 \vee (a_1 = a_2 \wedge (b_1 \preceq_2 b_2) \\ \qquad \wedge \\ a_2 \prec_1 a_1 \vee (a_2 = a_1 \wedge b_2 \preceq_2 b_1)\end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{l}a_1 \prec_1 a_2 \wedge a_2 \prec_1 a_1 \;\; \text{contrad.} \\ \qquad \vee \\ a_1 \prec_1 a_2 \wedge (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \;\; \text{contrad.} \\ \qquad \vee \\ (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \wedge a_2 \prec_1 a_1 \;\; \text{contrad.} \\ \qquad \vee \\ (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \wedge (a_2 = a_1 \wedge b_2 \preceq_2 b_1)\end{array}\right.$$

$$\begin{aligned}
&\Leftrightarrow \quad (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \wedge (a_2 = a_1 \wedge b_2 \preceq_2 b_1) \\
&\Leftrightarrow \quad a_1 = a_2 \wedge (b_1 \preceq_2 b_2 \wedge b_2 \preceq_2 b_1) \\
&\Leftrightarrow \quad a_1 = a_2 \wedge b_1 = b_2 \text{ por antisimetría de } \preceq_2 \\
&\Leftrightarrow \quad (a_1, b_1) = (a_2, b_2)
\end{aligned}$$

Transitiva

Sean $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$. Entonces

Orden lexicográfico

$$\begin{cases} (a_1, b_1) \preceq (a_2, b_2) \\ \qquad\quad \wedge \\ (a_2, b_2) \preceq (a_3, b_3) \end{cases} \Leftrightarrow \begin{cases} a_1 \prec_1 a_2 \vee (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \\ \qquad\quad \wedge \\ a_2 \prec_1 a_3 \vee (a_2 = a_3 \wedge b_2 \preceq b_3) \end{cases}$$

$$\Leftrightarrow \begin{cases} a_1 \prec_1 a_2 \wedge a_2 \prec_1 a_3 \\ \qquad\quad \vee \\ (a_1 \prec_1 a_2) \wedge (a_2 = a_3 \wedge b_2 \preceq_2 b_3) \\ \qquad\quad \vee \\ (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \wedge (a_2 \prec_1 a_3) \\ \qquad\quad \vee \\ (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \wedge (a_2 = a_3 \wedge b_2 \preceq_2 b_3) \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} (a_1 \prec_1 a_2 \wedge a_2 \prec_1 a_3) \\ \qquad \vee \\ (a_1 \prec_1 a_3 \wedge b_2 \preceq_2 b_3) \\ \qquad \vee \\ (a_1 \prec_1 a_3 \wedge b_1 \preceq_2 b_2) \\ \qquad \vee \\ (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \wedge (a_2 = a_3 \wedge b_2 \preceq_2 b_3) \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} (a_1 \prec_1 a_2 \wedge a_2 \prec_1 a_3) \\ \qquad \vee \\ (a_1 \prec_1 a_3) \wedge (b_2 \preceq_2 b_3 \vee b_1 \preceq_2 b_2) \\ \qquad \vee \\ (a_1 = a_2 \wedge b_1 \preceq_2 b_2) \wedge (a_2 = a_3 \wedge b_2 \preceq_2 b_3) \end{cases}$$

$$\Leftrightarrow \begin{cases} a_1 \prec_1 a_3 & \text{transitividad de } \prec_1 \\ \quad\vee & \\ a_1 \prec_1 a_3 & \\ \quad\vee & \\ a_1 = a_3 \wedge b_1 \preceq_2 b_3 & \text{transitividad de } \preceq_2 \end{cases}$$

$$\Leftrightarrow \quad a_1 \prec_1 a_3 \vee (a_1 = a_3 \wedge b_1 \preceq_2 b_3)$$

$$\Leftrightarrow \quad (a_1, b_1) \preceq (a_3, b_3)$$

Nota:

Si $(A, \preceq_1)$ y $(B, \preceq_2)$ son conjuntos totalmente ordenados, el orden lexicográfico en $A \times B$, es de la misma manera, totalmente ordenado.

Ejemplo

Sea $(\mathbb{R}, \leq)$, donde $\leq$ es el orden común. Sea $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. El orden lexicográfico en $\mathbb{R}^2$ se define como:

$$(x_1, y_1) \preceq (x_2, y_2) \Leftrightarrow x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 \leq y_2),$$

donde (x_1, y_1) y (x_2, y_2) son las coordenadas de dos puntos, p_1 y p_2 en $\mathbb{R}^2$.

En este caso, p_1 debe encontrarse en una recta vertical a la izquierda de otra recta vertical que contiene a p_2 o p_1 debe encontrarse por

debajo o en el mismo lugar de p_2 en la misma recta vertical, porque en cada línea vertical se sigue el orden de $\mathbb{R}$. Un punto p_1 de una recta vertical precede a cualquier punto p_2 de una recta vertical que esté a la derecha.

Definición

El orden lexicográfico extendido al producto cartesiano $A_1 \times A_2 \times \cdots \times A_n$ de define como:

$$(a_1, a_2, \ldots, a_n) \preceq (b_1, b_2, \ldots, b_n) \quad \Leftrightarrow \quad \begin{cases} a_1 \prec b_1 \\ \qquad \vee \\ a_1 = b_1 \wedge a_2 \prec b_2 \\ \qquad \vee \\ a_1 = b_1 \wedge a_2 = b_2 \wedge a_3 \prec b_3 \\ \qquad \vee \\ \ldots\ldots\ldots \\ \qquad \vee \\ a_1 = b_1 \wedge a_2 = b_2 \wedge a_3 = b_3 \wedge \cdots \\ \wedge\, a_{n-1} = b_{n-1} \wedge a_n \preceq b_n \end{cases}$$

El orden de prioridad empieza con la primera coordenada. Si la primera coordenada satisface la igualdad, se prueba la segunda. Si ésta también satisface la igualdad, se prueba la tercera y así sucesivamente.

Ejemplo

Consideremos el conjunto $A = \{a, b, c, \ldots, z\}$ con el orden alfabético común (orden total). El conjunto A^n (producto cartesiano) es el conjunto de todas las cadenas de n caracteres (longitud = n). Este concepto será abordado con más detalle en un próximo capítulo.

Si $p_1, p_2 \in A^n$ y $p_1 \preceq p_2$, entonces la palabra p_1 debe anteceder a la palabra p_2. Por ejemplo:

$$\text{andrógeno} \preceq \text{andrómeda},$$

porque los primeros cinco (5) caracteres son iguales, pero en el sexto caracter ocurre que “g $\preceq$ m”.

Es posible que las palabras p_1 y p_2 tengan diferentes longitudes, es decir, que pertenezcan productos cartesianos A^m y A^n, respectivamente. En este caso se usa el hecho de que toda palabra es mayor o igual que cualquiera de sus prefijos. Por ejemplo,

$$\text{pasa} \preceq \text{pasado}.$$

1. Sea $A = \{\text{Pedro, Juan, Luis, Jorge}\}$ y $R \subseteq A \times A$, definida por

$$\begin{aligned} R &= \{(\text{Juan, Pedro}), (\text{Pedro, Pedro}), (\text{Juan, Juan}), \\ &\quad (\text{Juan, Luis}), (\text{pedro, Jorge}), (\text{Luis, Luis}), \\ &\quad (\text{luis, pedro}), (\text{Jorge, Jorge})\}. \end{aligned}$$

   Determine si R es una relación de orden.

2. Sea $A = \mathbb{Z}$ y $R \subseteq A \times A$. Determine si las siguientes relaciones son de orden y el tipo de orden (parcial o total).
   a. $R = \{(x, y) \mid x = 2y\}$
   b. $R = \{(x, y) \mid x^2 \mid 2y\}$
   c. $R = \{(x, y) \mid \exists k \in \mathbb{Z}^+, x = y^k\}$

3. Sea $A = \{1, 2, 3, 4, 5, 6\}$ y $R \subseteq A \times A$, definida por

$$\begin{aligned} R &= \{(1,2),(1,3),(2,3),(1,1),(2,2),(3,3),(4,4),(4,6), \\ &\quad (5,6),(4,5),(5,5),(6,6)\}. \end{aligned}$$

   Determine si R es de orden. En caso afirmativo, verificar si es de orden total o parcial.

4. Sea $A = \mathbb{Z}^+$ y $R \subseteq A \times A$, definida por $R = \{(x, y) \mid x + n = y,\ n \in \mathbb{N}\}$. Pruebe que R es de orden total y buena ordenación. Si $A = \mathbb{Z}$, pruebe que es de orden total, pero no buena ordenación.

5. Sea $A = \{a, b, c, 7, 11\}$ y $R \subseteq A \times A$, definida por $R = \{(a, b), (b, c), (7, 11)\}$.

a. Completar la relación binaria R para que sea de orden.
b. Completar la relación binaria R para que sea reflexiva y transitiva, pero no simétrica ni antisimétrica.
c. Completar la relación de b para que sea de equivalencia.

6. Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ y $R \subseteq A \times A$, definida por

$$\begin{aligned} R = \{&(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(1,7),\\ &(1,8),(2,2),(2,5),(2,6),(2,8),(3,3),(3,5),(3,7),\\ &(3,8),(4,4),(4,6),(4,7),(4,8),(5,5),(5,8),(6,6),\\ &(6,8),(7,7),(7,8),(8,8)\} \end{aligned}$$

a. Compruebe que R es de orden en A.

b. Calcule máximo y mínimo del conjunto A para R.
c. Calcule los maximales y minimales del conjunto ordenado $B = A - \{1, 8\}$ para la relación inducida por R.
d. Calcule las cotas superiores e inferiores del conjunto ordenado $B = A - \{1, 8\}$ en A.
e. Represente gráficamente los conjuntos A y B.

7. Sean $S = \{1, 2, 3\}$ y $A = P(S)$. Dibuje el diagrama de Hasse del conjunto parcialmente ordenado $(A, \subseteq)$.
8. Sea $D_n = \{x \in \mathbb{Z}^+ \,|\, x \,|\, n \;\; (x \text{ divide a } \; n)\}$. Considere el conjunto $A = D_{30}$.
   a. Dibuje el diagrama de Hasse.
   b. Encuentre los elementos minimales y maximales.
   c. Halle los subconjuntos de A totalmente ordenados.

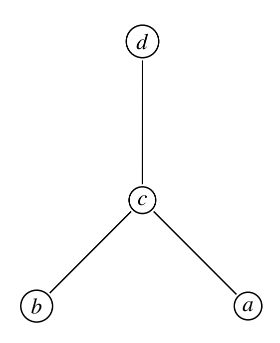
9. Considere el conjunto ordenado $(\mathbb{Z}^+ \times \mathbb{Z}^+, \preceq)$, donde $\preceq$ es el orden lexicográfico. Determine el valor de verdad de las siguientes proposiciones:
   a. $(3,4) \preceq (5,8)$
   b. $(5,4) \preceq (5,7)$
   c. $(2,10) \preceq (2,8)$
   d. $(8,9) \preceq (7,3)$
10. Sea $A = \{a,b,c,d\}$ y
    $R = \{(a,a),(a,b),(b,b),(b,d),(a,c),(c,c),(c,d),(a,d),(d,d)\}$.
    Determine el diagrama de Hasse.

11. Sea $A = \{1, 2, 3, 4, 5\}$ y

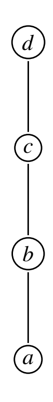
$$R = \{(1,1),(2,2),(3,3),(1,3),(3,4),(3,5),(1,4),(4,4),(1,5),(2,3),(2,4),(2,5),(5,5)\}.$$

Determine el diagrama de Hasse.

12. Describir las parejas ordenadas de la relación determinada por el diagrama de Hasse siguiente en el conjunto $A = \{a, b, c, d\}$.



13. Describir las parejas ordenadas de la relación determinada por el diagrama de Hasse siguiente en el conjunto $A = \{a, b, c, d\}$.



14. Encuentre el diagrama de Hasse de la relación en el conjunto $A = \{1, 2, 3, 4, 5\}$, cuya representación matricial es:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

15. Encuentre los diagramas de Hasse de los conjuntos siguientes ordenados por la relación de divisibilidad y diga cuáles están totalmente ordenados.
   a. $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$
   b. $A = \{2, 4, 8, 16, 32\}$

c. $A = \{3, 6, 12, 36, 72\}$
d. $A = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 30, 60\}$

El orden topológico consiste en encontrar un orden total $\prec$ en un conjunto parcialmente ordenado $(A, \preceq)$, preservando siempre el orden parcial. Este concepto es sumamente importante en ciencias computacionales cuando necesitamos introducir conjunto de datos a la computadora, los cuales deben estar ordenados. Es importante hacer notar que la extensión de un conjunto parcialmente ordenado a un conjunto totalmente ordenado no es única. Es decir, de un mismo conjunto parcialmente ordenado se puede construir uno o más conjuntos totalmente ordenados. Por ejemplo, consideremos el conjunto parcialmente ordenado:

$$A = \{(a,b),(a,c),(a,d),(b,e),(d,e),(e,f),(c,g),(g,f)\}.$$

El conjunto $B = \{(a, b), (b, c), (c, d), (d, e), (e, g), (g, f)\}$ es un conjunto totalmente ordenado. De igual forma, los conjuntos
$D = \{(a, c), (c, g), (g, b), (b, d), (d, e), (e, f)\}$ y
$E = \{(a, d), (d, b), (b, e), (e, c), (c, g), (g, f)\}$.

Algoritmo del orden topológico

El objetivo es construir una cadena de la forma:

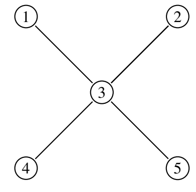
$$a_1 \preceq a_2 \preceq \cdots \preceq a_n,$$

donde $a_1, a_2, \ldots, a_n$ son los elementos minimales de los conjuntos considerados en cada paso.

El algoritmo empieza tomando cada elemento minimal del conjunto original y luego se excluye del mismo. Luego, de sacar los elementos minimales del conjunto inicial, se hace lo mismo con los elementos minimales del conjunto que queda y así sucesivamente hasta concluir con todos los elementos del conjunto.

Ejemplo

Sea $A = \{1, 2, 3, 4, 5\}$. Considere el orden parcial del conjunto $(A, \preceq)$ representado por el siguiente diagrama de Hasse:



Determine un orden total de este conjunto.

Solución

Observemos que el 4 es un elemento minimal, se excluye y queda el conjunto $\{1, 2, 3, 5\}$. El 5 es un elemnto minimal de este conjunto, se excluye y queda el conjunto $\{1, 2, 3\}$. De este conjunto, el 3 es

minimal, se excluye y queda el conjunto $\{1, 2\}$. El 1 y 2 son minimales de este útimo conjunto. Por tanto, los órdenes totales son:

$$4 \preceq 5 \preceq 3 \preceq 2 \preceq 1.$$

y

$$4 \preceq 5 \preceq 3 \preceq 1 \preceq 2.$$

1. Considere los conjuntos parcialmente ordenados del item 15 del grupo de ejercicios anteriores. Encuentre un orden total en cada uno.
2. Sea $S = \{a, b, c\}$ y $A = P(S)$. Considere el conjunto $(A, \subseteq)$. Encuentre un orden total.

Contenido

Definición

Sean A y B conjuntos no vacíos. Una **Función** $f : A \to B$ es una relación de A a B que asigna a determinados elementos de A un único elemento de B. Es decir, si no hay primeras componentes repetidas en los pares ordenados que forman la relación.
Se escribe $f(a) = b$ para indicar que $(a, b) \in f$. A b se le llama **imagen** de a en f y a a se le llama **precedente o antecedente** de b.

El conjunto de los elementos $x \in A$ que tienen imagen en B se le llama **Dominio de definición** de la función f y es claro que es subconjunto de A. Cuando el dominio de definición de f es igual a A, se dice que la función es una **Aplicación**.

El conjunto de los elementos $y \in B$ que son imágenes de elementos $x \in A$ se le llama **Domino de imágenes o imagen** de la función f y es evidente que es subconjunto de B.

Ejemplo 1

Sean $A = \{a, b, c\}$ y $B = \{3, 4, 5, 6\}$.

Entonces $f = \{(a, 3), (b, 4), (c, 4)\}$ es una función. Ahora bien, la relación $R_1 = \{(a, 3), (b, 3), (b, 4)\}$ no es una función, ya que el mismo precedente b tiene dos imágenes.

Observe que podemos escribir:
$f(a) = 3, \quad f(b) = 4, \quad f(c) = 4, \quad f(A) = \{3, 4\}$

Ejemplo 2

Sea $f : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = x^2$. Esta función tiene como dominio y codominio al conjunto $\mathbb{R}$. f asigna a cada número real su cuadrado. En este caso, la imagen de f, $f(\mathbb{R}) = [0, +\infty)$.

Sea $f : \mathbb{R} \to B$, donde $B = \{-1, 1\}$, tal que

$$f(x) = \begin{cases} 1, & \text{si } x \in \mathbb{Q} \\ -1, & \text{si } x \in \mathbb{I} \end{cases}$$

Entonces $f(\mathbb{R}) = B$. En lo adelante a los conjuntos A y B en la función $f : A \to B$ les llamaremos **Dominio de definición o simplemente Dominio** y **Codominio**, respectivamente de la función f. Al subconjunto de B formado por los elementos que aparecen como segunda componente en los pares ordenados que definen a f

se le llama **Dominio de imágenes o simplemente Imagen** de f y se representa por $f(A)$.

En el ejemplo 1 de esta sección, se tiene que el dominio de f, $D_f = \{a, b, c\}$, el codominio de f, $C_f = \{3, 4, 5, 6\}$ y la imagen de f, $f(A) = \{3, 4\}$.

Sean $A = \{a_1, a_2, \ldots, a_m\}$ y $B = \{b_1, b_2, \ldots, b_n\}$. Entonces $|A| = m$ y $|B| = n$. Una función $f : A \to B$ normalmente tiene la forma $\{(a_i, b_j) \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$. Para cada $a_i,\ i = 1, 2, \ldots, m$, cualquiera de los $b_j,\ j = 1, 2, \ldots, n$ es posible. Es decir que para cada a_i, hay como segunda componente, n posibilidades que son las n b_j.

Entonces por el principio del producto, se tiene que se pueden construir

$$n^m = |B|^{|A|}$$

funciones $f : A \to B$.

Para los conjuntos del ejemplo 1, se tiene que hay

$$|B|^{|A|} = 4^3 = 64$$

funciones $f : A \to B$.

Ejemplo 3

Sean $A = \{a, b, c\}, \;\; B = \{3, 4\}$. Entonces hay $|B|^{|A|} = 2^3 = 8$ funciones $f : A \to B$. Estas funciones son:

$$\{(a,3),(b,3),(c,3)\},\; \{(a,3),(b,3),(c,4)\},\; \{(a,3),(b,4),(c,3)\},$$

$$\{(a,3),(b,4),(c,4)\},\; \{(a,4),(b,3),(c,3)\},\; \{(a,4),(b,3),(c,4)\},$$
$$\{(a,4),(b,4),(c,3)\},\; \{(a,4),(b,4),(c,4)\}$$

Definición

Dos funciones f y g son **Iguales** ($f = g$) si:

a. tienen el mismo dominio A.

b. $f(a) = g(a), \;\; \forall a \in A$

Ejemplo 4

Sean $A = \{2, 4, 6\}$, $B = \{1, 2, 3, 4\}$, $f : A \to B$ tal que $f = \{(2, 1), (4, 2), (6, 3)\}$ y $g : A \to B$ tal que $g(x) = 2|x$. Es claro que $f = g$, puesto que tienen el mismo dominio A y asignan el mismo elemento de B a cada elemento de A.

Definición

Sean A y B conjuntos. Una función $f : A \to B$ se llama **Constante**, si a cada elemento $a \in A$ se le asigna el mismo elemento $b \in B$. Es decir, si $f(A)$ consta de un solo elemento.

Ejemplo 5

Sean $A = \{a, b, c\}, \ \ B = \{3, 4, 5\}$ y $f : A \to B$ tal que $f = \{(a, 4), (b, 4), (c, 4)\}$. Se observa que a cada elemento de A se le asigna el mismo elemento de B. En este caso, el 4. Por tanto, f es constante.

Definición

Sean A y B conjuntos no vacíos. Una función $f : A \to B$ es **Inyectiva** o **Uno a Uno** si elementos diferentes de A, tienen imágenes distintas.

Sean A y B conjuntos finitos . Si $f : A \to B$ es inyectiva, entonces $|A| \leq |B|$.

Otra forma de caracterizar las funciones inyectivas es:

$$\forall x, y \in A : x \neq y \Rightarrow f(x) \neq f(y)$$

o

$$\forall x, y \in A : f(x) = f(y) \Rightarrow x = y.$$

Ejemplo 6

Sean $A = \{3, 4, 5\}$ y $B = \{3, 4, 5, 6, 7\}$. Entonces la función $f : A \to B$ tal que

$$f = \{(3, 4), (4, 6), (5, 3)\}$$

es inyectiva. Sin embargo, la función $g : A \to B$ tal que

$$g = \{(3, 3), (4, 5), (5, 3)\}$$

no es inyectiva, por que siendo $3 \neq 5$ se tiene que $g(3) = g(5)$.

Existe la prueba de la **Recta horizontal** que dice que una función es inyectiva, si su gráfica no corta en más de un punto esta recta.

Ejemplo 7

Sea $f : \mathbb{R} \to \mathbb{R}$ una función definida por $f(x) = 2x + 3$. Probemos que f es inyectiva.

Prueba

Probemos que si $f(x_1) = f(x_2)$, entonces $x_1 = x_2$. Entonces tomemos la expresión

$$2x_1 + 3 = 2x_2 + 3 \Rightarrow 2x_1 = 2x_2 \Rightarrow x_1 = x_2.$$

Luego, f es inyectiva.

Ejemplo 8

Sea $f : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = x^3$. Esta función es inyectiva porque el cubo de dos números reales diferentes son diferentes.

Sean $A = \{a_1, a_2, \ldots, a_m\}$ y $B = \{b_1, b_2, \ldots, b_n\}$ con $m \leq n$. Entonces $|A| = m$ y $|B| = n$. Una función $f : A \to B$ normalmente tiene la forma $\{(a_i, b_j) \,|\, 1 \leq i \leq m, \;\; 1 \leq j \leq n\}$. Entonces a_1 se puede acompañar de cualquiera de las n posibles selecciones de los b_j (segunda componente), a_2 se puede acompañar de las $n - 1$ posibles selecciones de los b_j que quedan y así sucesivamente hasta llegar a que a_m se puede acompañar de $n - (m - 1) = n - m + 1$ selecciones

posibles de los b_j. Entonces por el principio del producto, se tiene que el número de funciones inyectivas $f : A \to B$ viene dado por

$$n(n-1)(n-2)\cdots(n-m+1) = \frac{n!}{(n-m)!} = P(n,m) = P(|B|,|A|).$$

En el caso del ejemplo 6, se tiene que la cantidad de funciones inyectivas es

$$P(5,3) = \frac{5!}{(5-3)!} = \frac{5!}{2!} = 5 \times 4 \times 3 = 60.$$

Definición

Sean A y B conjuntos no vacíos. Si $f : A \to B$ y $A_1 \subseteq A$, entonces

$$f(A_1) = \{b \in B | f(a) = b \text{ para algún } a \in A_1\}.$$

Teorema

Sea A un conjunto no vacío. Sean $A_1 \subseteq A$ y $A_2 \subseteq A$ y sea $f : A \to B$. Entonces

a. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
b. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.
c. $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$, si f es inyectiva.

Demostración

Prueba del apartado **a**. Las demás se dejan como ejercicios.

Debemos probar que:

1. $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$
2. $f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2)$.

Prueba de 1.

Sea $b \in f(A_1 \cup A_2)$. Entonces $\exists a \in A_1 \cup A_2 \ni (f(a) = b,\ a \in A_1)$ o $(f(a) = b,\ a \in A_2)$. Entonces $b \in f(A_1)$ o $b \in f(A_2)$. Entonces $b \in f(A_1) \cup f(A_2)$. Luego,

$$f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$$

Prueba de 2.

Sea $b \in f(A_1) \cup f(A_2)$. Entonces $b \in f(A_1)$ o $b \in f(A_2)$.
Entonces $\exists a \ni (a \in A_1, f(a) = b)$ o $(a \in A_2, f(a) = b)$.
Entonces $a \in A_1 \cup A_2,\ f(a) = b \in f(A_1 \cup A_2)$.
Luego,

$$f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2).$$

Esto completa la prueba.

Definición

Sea A un conjunto no vacío. Sea $A_1 \subseteq A$ y sea $f : A \to B$. Se llama **Restricción** de f a A_1 a la función $f|A_1 : A_1 \to B$ tal que $f|A_1(a) = f(a), \ \forall a \in A_1$.

Definición

Sea A un conjunto no vacío. Sea $A_1 \subseteq A$ y sea $f : A_1 \to B$. Si $g : A \to B$ y $g(a) = f(a), \ \forall a \in A_1$, se dice que g es una **Extensión** de f a A.

Ejemplo 9

Sean $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4, 5\}$, y $A_1 = \{a, c, d\}$. Sean $f : A \to B$ tal que $f = \{(a, 1), (b, 3), (c, 5), (d, 4)\}$ y $g : A_1 \to B$ tal que $g = \{(a, 1), (c, 5), (d, 4)\}$. Es claro que $g = f|A_1$ es una restricción de f a A_1 y f una extensión de g de A_1 a A.

Definición

Sean A y B dos conjuntos no vacíos. Una función $f : A \to B$ es **Sobreyectiva** si $f(A) = B$. Es decir, si para cada elemento $b \in B$, $\exists a \in A \ni f(a) = b$.

Ejemplo 10

Sean $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$ y $f : A \to B$ tal que $f = \{(a, 3), (b, 2), (c, 1), (d, 2)\}$. Es claro que esta función es

sobreyectiva, porque cada elemento de B es imagen de al menos un elemento de A.

La función $g : A \to B$ tal que $g = \{(a, 1), (b, 1), (c, 2), (d, 2)\}$ no es sobreyectiva, porque hay elementos de B que no son imagen.

Ejemplo 11

La función $f : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = x^3$ es sobreyectiva. Sin embargo, la función $g : \mathbb{R} \to \mathbb{R}$ tal que $g(x) = x^2$ no es sobreyectiva, puesto que $g(\mathbb{R}) = [0, +\infty) \subset \mathbb{R}$.

Si A y B son conjuntos finitos, debe ocurrir que $|A| \geq |B|$ para que haya una función sobreyectiva $f : A \to B$.

Si A y B son conjuntos finitos con $|A| = m$, $|B| = n$ y $m \geq n$, entonces la cantidad de funciones sobreyectivas $f : A \to B$ viene dada por

$$\sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^m.$$

Ejemplo 12

Sea $B = \{x \in \mathbb{N} \,|\, x = 2k,\ k \in \mathbb{N}\}$ y sea $f : \mathbb{N} \to B$ tal que $f(x) = 2x$. Esta función es sobreyectiva, ya que todo elemento de B es imagen. Sin embargo, la función $f : \mathbb{N} \to \mathbb{N}$, tal que $f(x) = 2x$ no es sobreyectiva, puesto que hay elementos en $\mathbb{N}$ que no son imágenes de algún elemento de $\mathbb{N}$.

Ejemplo 13

La función $f:\mathbb{R}\to[0,+\infty)$, tal que $f(x)=x^2$ es sobreyectiva. Observe que la función $f:\mathbb{R}\to\mathbb{R}$, tal que $f(x)=x^2$ no es sobreyectiva.

Ejemplo 14

Sea $f:\mathbb{R}\to\mathbb{R}$, tal que $f(x)=3x-5$. Probar que es sobreyectiva. Tomemos $y\in\mathbb{R}$. $y=3x-5\Rightarrow x=(y+5)/3\in\mathbb{R}$. Ahora comprobamos que el x encontrado devuelve a y. $f((y+5)/3)=3(y+5)/3-5=y$. Esto demuestra que f es sobreyectiva.

Ejercicios

1. Sean A y B dos conjuntos finitos, tales que $|A| \geq 4$ y $|B| \geq 4$. Sea $f : A \to B$. Escriba un ejemplo de:
   a. f no sea inyectiva ni sobreyectiva
   b. f sea inyectiva y no sobreyectiva
   c. f sea sobreyectiva y no inyectiva
   d. f sea sobeyectiva e inyectiva
2. Sea $f : \mathbb{Z} \to \mathbb{Z}$. Diga cuáles de las siguientes funciones son inyectivas y cuáles son sobreyectivas. Determine la imagen $f(\mathbb{Z})$ de las que no son sobreyectivas.

a.	$f(x) = x + 7.$	b.	$f(x) = 2x - 3.$	c.	$f(x) = -x + 5.$
d.	$f(x) = x^2.$	e.	$f(x) = x^2 + x.$	f.	$f(x) = x^3.$

3. Sea $f : \mathbb{R} \to \mathbb{R}$. Diga cuáles de las siguientes funciones son inyectivas y cuáles son sobreyectivas. Determine la imagen $f(\mathbb{R})$ de las que no son sobreyectivas.

a.	$f(x) = x + 7.$	b.	$f(x) = 2x - 3.$	c.	$f(x) = -x + 5.$
d.	$f(x) = x^2.$	e.	$f(x) = x^2 + x.$	f.	$f(x) = x^3.$

4. Sean $A = \{a, b, c, d\}$ y $B = \{a, b, c, d, e, f\}$. Responda las siguientes preguntas:
   a. ¿Cuántas funciones hay de A a B?
   b. ¿Cuántas funciones inyectivas hay de A a B?
   c. ¿Cuántas funciones sobreyectivas hay de A a B?
   d. ¿Cuántas funciones hay de B a A?
   e. ¿Cuántas funciones inyectivas hay de B a A?
   f. ¿Cuántas funciones sobreyectivas hay de B a A?

5. Si $|A| = m = 2, 3, 4$ y $|B| = n = 5$. Verifique que

$$\sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^m = 0.$$

6. Un maestro constructor que desarrolla un proyecto habitacional, tiene 5 ayudantes. Necesita realizar 9 tareas. ¿De cuántas maneras puede el maestro constructor asignar estas tareas a los 5 ayudantes para que cada uno trabaje al menos en una?.
7. Pruebe que $f : (-\infty, -1] \to \mathbb{R}$, tal que

$$f(x) = 1 - \sqrt{x^2 - 4x - 5}$$

es inyectiva.

8. Determine si $f : \mathbb{R} \to \mathbb{R}$, tal que $f(x) = 2 - 4x - x^2$ es inyectiva, si no lo es, encuentre el intervalo para que lo sea.
9. Sea f una función definida por

$$f(x) = \begin{cases} \frac{1}{2}x^2 + 1, & x \in [-4, -2) \\ \sqrt{2 + x}, & x \in [-2, 2] \\ 1 - \frac{x}{2}, & x \in (2, 6] \end{cases}.$$

   Determine si es inyectiva.
10. ¿Cuáles de las siguientes funciones son sobreyectivas?
    a. $f : [0, +\infty) \to \mathbb{R} \ \ni f(x) = \sqrt{x}$
    b. $f : [-1, 2] \to [0, 4] \ \ni f(x) = x^2$
    c. $f : \mathbb{R} \to [0, +\infty) \ \ni f(x) = |x|$

d. $f : \mathbb{R} - \{0\} \to [-1, 1] \ \ni f(x) = \dfrac{|x|}{x}$

11. Determine si la función $f : \mathbb{R} - \{-5\} \to \mathbb{R}$, tal que $f(x) = \dfrac{x-5}{x+5}$ es inyectiva.
12. Sea $f : \mathbb{R} \to B$, tal que $f(x) = |x-2| - x$ una función sobreyectiva. Encuentre el conjunto B.

Definición

Ahora que conocemos el concepto de función, podemos redefinir algunos conceptos previos. Sea A un conjunto. Una función $f : A \times A \to A$ se le llama **Operación binaria** en A. Por ejemplo, la función $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $f(a, b) = a + b$ es una operación binaria en $\mathbb{N}$.

Si A es un conjunto y $f : A \times A \to A$, entonces

a. f es **Asociativa** si $\forall a, b, c \in A,\ f(f(a, b), c) = f(a, f(b, c))$.

b. f es **Conmutativa** si $\forall (a, b) \in A \times A,\ f(a, b) = f(b, a)$.

Definición

Sean A y B dos conjuntos y $D \subseteq A \times B$. La función $\pi_A : D \to A$ definida por $\pi_A(a, b) = a$ se le llama **Proyección** de D sobre la primera coordenada. De manera similar se puede definir π_B.
Es claro que si $D = A \times B$ se tiene que tanto π_A como π_B son sobreyectivas.

Generalizando, sean $A_1, A_2, A_3, \ldots, A_n$ conjuntos y sea $\{k_1, k_2, \ldots, k_m\} \subseteq \{1, 2, 3, \ldots, n\}$ siendo $k_1 < k_2 < \cdots < k_m$, $m \leq n$, para $D \subseteq A_1 \times A_2 \times A_3 \times \cdots \times A_n$, la función $\pi : D \to A_{k_1} \times A_{k_2} \times A_{k_3} \times \cdots \times A_{k_m}$, definida por $\pi(a_1, a_2, a_3, \ldots, a_n) = (a_{k_1}, a_{k_2}, a_{k_3}, \ldots, a_{k_m})$ es una **Proyección** de D sobre las k_1-ésima, k_2-ésima, k_3-ésima, ..., k_m-ésima coordenadas.

Ejemplo

Consideremos la relación $R \subseteq A_1 \times A_2 \times A_3 \times A_4 \times A_5 \times A_6$, donde los conjuntos se definen de la manera siguiente:

a. A_1 = Conjunto de códigos de empleado.
b. A_2 = Conjunto de códigos de departamento.
c. A_3 = Conjunto de nombres de empleado.
d. A_4 = Conjunto de nombres de cargo.
e. A_5 = Conjunto de códigos de nivel.
f. A_6 = Conjunto de códigos de categoría.

La relación R está definida mediante la tabla

C.Empl	C.Depto	Nombre	Cargo	Nivel	Cat
1000	2010	J. Valdez	Supervisor	8	F
1010	2010	A. Pérez	Asistente	10	F
1020	2000	M. Bentoso	Gerente	14	F
1030	3000	R. Montero	Gerente	13	F
1040	3010	S. Puello	Ayudante	9	T
1050	3010	M. Soto	Asistente	10	C
1060	4000	E. Bueno	Director	16	F
1070	4020	T. Torres	Supervisor	7	C
1080	4020	P. Victoria	Ing.Asesor	11	T
1090	4010	B. Basora	Asistente	10	T
1100	5000	D. Piedra	Director	18	F

El cuadro anterior es un ejemplo de lo que se llama **Tabla de una base de datos relacional**. A los conjuntos A_1, A_2, A_3, A_4, A_5 y A_6 se le suele llamar **Dominios de la base de datos relacional** . El número de colunnas de la tabla representa lo que se llama el grado de la tabla. A los elementos de R se les llama **Lista**.

Si queremos la proyección de R sobre $A_2 \times A_4 \times A_5$ se tiene la tabla

C.Depto	Cargo	Nivel
2010	Supervisor	8
2010	Asistente	10
2000	Gerente	14
3000	Gerente	13
3010	Ayudante	9
3010	Asistente	10
4000	Director	16
4020	Supervisor	7
4020	Ing.Asesor	11
4010	Asistente	10
5000	Director	18

Definición

Sean A y B conjuntos. Una función $f : A \to B$ es **Biyectiva**, si es inyectiva y sobreyectiva al mismo tiempo.

Ejemplo

Sean $A = \{a, b, c, d\}$ y $B = \{3, 4, 5, 6\}$. La función $f : A \to B$ definida por

$$f = \{(a, 3), (b, 4), (c, 5), (d, 6)\}$$

es biyectiva.

Definición

Sea A un conjunto. Una función $I_A : A \to A$ definida por $I_A(a) = a, \ \forall a \in A$ se le llama **Función identidad**. Esta función es biyectiva para cualquier conjunto A. Es claro que si $f : A \to A$ es biyectiva, entonces $f(A) = A$ y se dice que $f = \{(a, f(a))|a \in A\}$ es una **Permutación** de A.

Definición

Sean A, B y C conjuntos y $f : A \to B$, $g : B \to C$. La **Función compuesta** de g y f, representada por $g \circ f : A \to C$, se define como $(g \circ f)(a) = g(f(a)), \ \forall a \in A$.

Ejemplo

Sean $A = \{a, b, c, d\}, \;\; B = \{1, 2, 3\}$ y $C = \{5, 6, 7, 8\}$. Sean $f : A \to B$, definida por $f = \{(a, 1), (b, 1), (c, 2), (d, 3)\}$, $g : B \to C$, definida por $g = \{(1, 6), (2, 7), (3, 8)\}$. La función compuesta viene dada por

$$g \circ f = \{(a, 6), (b, 6), (c, 7), (d, 8)\}.$$

Ejemplo

Sean $f : \mathbb{R} \to \mathbb{R}$ y $g : \mathbb{R} \to \mathbb{R}$, definidas por $f(x) = x - 7$ y $g(x) = x^3$. Entonces

$$(g \circ f)(x) = g(f(x)) = (x - 7)^3$$

y

$$(f \circ g)(x) = f(g(x)) = x^3 - 7.$$

Teorema

Sean A y B conjuntos y $f : A \to B$, $g : B \to C$. Entonces

a. Si f y g son inyectivas, se tiene que $g \circ f$ es inyectiva
b. Si f y g son sobreyectivas, se tiene que $g \circ f$ es sobreyectiva

Demostración

a. Debemos probar que $g \circ f : A \to C$ es inyectiva. Sean $x_1, x_2 \in A$, tal que $(g \circ f)(x_1) = (g \circ f)(x_2)$. Entonces
$(g \circ f)(x_1) = (g \circ f)(x_2) \Leftrightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2)$, porque g es inyectiva. Como f es inyectiva, se tiene que $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. Luego, $g \circ f$ es inyectiva.

b. Debemos probar que $g \circ f : A \to C$ es sobreyectiva. Sea $t \in C$. Como g es sobreyectiva, $\exists\, s \in B$, tal que $g(s) = t$. Como f es sobreyectiva, $\exists\, x \in A$ tal que $f(x) = s$. Entonces $t = g(s) = g(f(x)) = (g \circ f)(x)$. Como t es arbitrario en C, se tiene que la imagen de $g \circ f$ es C y $g \circ f$ es sobreyectiva. ■

Definición

Sea A un conjunto y $f : A \to A$. Las potencias de f se definen recursivamente de la siguiente manera:

a. $f^1 = f$

b. $f^{n+1} = f \circ f^n$, para $n \in \mathbb{Z}^+$

Ejemplo

Sea $A = \{a, b, c, d\}$ y $f : A \to A$, tal que $f = \{(a, b), (b, b), (c, a), (d, c)\}$. Entonces

$$f^2 = f \circ f = \{(a, b), (b, b), (c, b), (d, a)\}$$
$$f^3 = f \circ f^2 = \{(a, b), (b, b), (c, b), (d, b)\}.$$

La composición de funciones satisface la propiedad asociativa. De modo que

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$$

y

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))).$$

Observación: La notación usada para la composición de funciones es ligeramente diferente a la utilizada en la composición de relaciones, en cuanto al orden de la simbología.

Definición

Sean A y B conjuntos. Sea $f : A \to B$ una función. La **Inversa** de f, denotada por $f^{-1} : B \to A$ se define como $f^{-1} = \{(b, a)|(a, b) \in f\}$. Es claro que la inversa de una función no es necesariamente una función, como lo muestra el siguiente ejemplo:

Sean $A = \{a, b, c\}$ y $B = \{3, 4, 5\}$. Sea $f : A \to B$ definida por $f = \{(a, 3), (b, 4), (c, 4)\}$. Entonces $f^{-1} : B \to A$ tal que $f^{-1} = \{(3, a), (4, b), (4, c)\}$ es una relación, pero no una función.

Si la inversa de una función f es una función se le llama **Función inversa** (f^{-1}). Es evidente que

$$f^{-1} \circ f = I_A \text{ y } f \circ f^{-1} = I_B.$$

Ejemplo

La inversa de la función $f(x) = 2x + 3$ es la función

$$f^{-1}(x) = \frac{x-3}{2}.$$

Ejemplo

La inversa de la función $f(x) = \dfrac{2x-5}{4}$ es la función

$$f^{-1}(x) = \frac{4x+5}{2}.$$

Ejemplo

La inversa de la función

$$f(x) = \frac{x+3}{x-2}$$

es la función

$$f^{-1}(x) = \frac{2x+3}{x-1}.$$

Ejemplo

La función $f(x) = x^2$ no tiene función inversa, ya que su inversa es

$$f^{-1}(x) = \pm\sqrt{x}$$

y esta no es función.

Ejemplo

La inversa de la función $f(x) = \sqrt[3]{x+2}$ es la función

$$f^{-1}(x) = x^3 - 2.$$

Definición

Sean A y B conjuntos y $f : A \to B$. Decimos que f es invertible, si existe una función $g : B \to A$ tal que $g \circ f = I_A$ y $f \circ g = I_B$.

Ejemplo

Sean $f : \mathbb{R} \to \mathbb{R}$ y $g : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = 5x + 3$ y $g(x) = \dfrac{x-3}{5}$. Entonces

$$(g \circ f)(x) = g(f(x)) = g(5x + 3) = \frac{5x + 3 - 3}{5} = x$$

y

$$(f \circ g)(x) = f(g(x)) = f\left(\frac{x-3}{5}\right) = 5\left(\frac{x-3}{5}\right) + 3 = x.$$

Luego, $f \circ g = I_{\mathbb{R}}$ y $g \circ f = I_{\mathbb{R}}$. Por tanto, f y g son invertibles.

Teorema

Sean A y B conjuntos y $f : A \to B$. Si f tiene función inversa, ésta es única.

Demostración

Vamos a suponer que hay dos funciones inversas, $g : B \to A$ y $h : B \to A$. Entonces $g \circ f = I_A, \;\; f \circ g = I_B$ y $h \circ f = I_A, \;\; f \circ h = I_B$. Ahora tenemos que $h = h \circ I_B = h \circ (f \circ g) = (h \circ f) \circ g = I_A \circ g = g$. Luego, la inversa de una función es única. ■

Teorema

Sean A y B conjuntos. La función $f : A \to B$ tiene función inversa, si y sólo si, es inyectiva y sobreyectiva.

Demostración

a. Supongamos que f tiene la función inversa $g : B \to A$. Entonces $g \circ f = I_A, \ \ f \circ g = I_B$. Sean $x_1, x_2 \in A$ tales que $f(x_1) = f(x_2)$. Entonces $g(f(x_1)) = g(f(x_2))$. Es lo mismo decir que $(g \circ f)(x_1) = (g \circ f)(x_2)$. Ahora bien, como $g \circ f = I_A$, se tiene que $x_1 = x_2$ y f es inyectiva. Ahora probaremos que f es sobreyectiva.

Sea $y \in B$. Entonces $g(y) \in A$ y por tanto, existe $f(g(y))$. Ahora bien, como $f \circ g = I_B$, se tiene que $y = I_B(y) = (f \circ g)(y) = f(g(y))$, lo que muestra que f es sobreyectiva.

b. Supongamos ahora que f es biyectiva. Debemos probar que f tiene inversa.

Como f es sobreyectiva, $\forall b \in B, \;\; \exists a \in A \;\; \ni f(a) = b$. Luego, definamos la función $g : B \to A$ tal que $g(b) = a$, donde $f(a) = b$. Es claro que g es única. Como f es inyectiva, elementos diferentes en A producen imágenes diferentes en B. Por tanto, como hemos definido a g de modo tal que $g \circ f = I_A, \;\; f \circ g = I_B$, se tiene que g es la inversa de f. ■

Contenido

Principio del palomar

Si m objetos se colocan en n cajas, donde $m > n$, entonces hay al menos una caja que contiene dos o más objetos.

Ejemplo

En una empresa hay 32 empleados que cumplen año en Enero. Entonces hay al menos dos empleados que cumplen año el mismo día.

Ejemplo

Un Señor le pasa al limpiabotas una funda con 7 pares de zapatos, donde cada par es de diferente color. Si se sacan al azar de la funda, para obtener un par del mismo color, debe extraer por menos 8 zapatos.

1. Sea $A = \{1, 2, 3, 4\}$ y sea $R : A \to A$. Determine cuáles de las relaciones siguientes son funciones.
   a. $R = \{(2, 3), (1, 4), (2, 1), (3, 2), (4, 4)\}$
   b. $R = \{(3, 1), (4, 2), (1, 1)\}$
   c. $R = \{(2, 1), (3, 4), (1, 4), (2, 1), (4, 4)\}$
   d. $R = \{(2, 3), (1, 6), (4, 2), (3, 4)\}$
2. Sean $A = \{1, 2, 3, 4, 5, 6\}, \quad B = \{1, 2, 3, 4\}$ y $f : A \to B$ definida por $f = \{(1, 2), (2, 4), (3, 3), (4, 1), (5, 2), (6, 4)\}$. Determine:
   a. $f(2), \quad f(4), \quad f(6)$
   b. $f^{-1}(2), \quad f^{-1}(3), \quad f^{-1}(4)$
   c. $\{x|x \in A, \ f(x) < 3\}$
3. ¿Qué se necesita para que el conjunto $f = \{(1, 5), (3, 1), (4, 7), (-2, -3)\}$ sea una función de A a B?.

4. Sea $S = \{1, 2, 3, 4\}$ y $f : S \to S$, una función inyectiva y sobreyectiva definida por $f = \{(1, 2), (2, 4), (3, 1), (4, 3)\}$. Encuentre f^{-1}.
5. Sea $A = \{1, 2, 3, 4\}$ y $f, g : A \to A$ definidas por $f = \{(1, 2), (2, 1), (3, 5), (4, 4), (5, 2)\}$, $g = \{(1, 1), (2, 3), (3, 5), (4, 3), (5, 1)\}$. Determine
   a. $f(3)$, $g(5)$, $f^{-1}(2)$, $g^{-1}(1)$, $f^{-1}(4)$, $g \circ f$, $f \circ g$
   b. $f^{-1}(\{1, 2\})$, $\{x|f(x) \leq 4\}$, $\{x|g(x) > 2\}$

6 Sea $f : A \to B$ una función representada por medio de un diagrama de coordenadas de $A \times B$. ¿Qué propiedad geométrica tiene f, si :
   a. f es inyectiva
   b. f es constante
   c. f es sobreyectiva

d. Si f tiene una inversa f^{-1}

7 Sombree en un sistema de coordenadas cartesiano cada una de las siguientes regiones R:

a. $R = \{x| -3 < x \leq 2\} \times \{x| -2 < x < 4\}$
b. $R = \{x||x| < 3\} \times \{x||x| \leq 1\}$
c. $R = \{x||x| \leq 2\} \times \{x|x > -3\}$

8. Represente gráficamente cada una de las siguientes funciones $f : \mathbb{R} \to \mathbb{R}$:

a. $f(x) = 4x - x^2$

b. $f(x) = x + 2|x|$

c. $f(x) = \begin{cases} x^2, & x \geq 0 \\ 1 - x, & x < 0 \end{cases}$

d. $f(x) = \begin{cases} 3 - x, & x > 0 \\ x, & |x| \leq 2 \\ 2, & x < -2 \end{cases}$

9. Sean $A = \{\text{Antonio}, \text{Pedro}, \text{Luis}\}$ y $B = \{\text{Pedro}, \text{David}, \text{Pablo}, \text{Juan}\}$. Encunetre
   a. $A \times B$ b. $B \times A$ c. $A \times A$.
10. Represente en un sistema de coordenadas cartesiano las áreas definidas por los siguientes productos:
    a. $[-3, 3] \times [-1, 2]$ b. $]-2, 3] \times [-3, +\infty[$
    c. $[-3, 1[\times] - \infty, 2]$
11. Sean $A = \{2, 3\}$, $B = \{1, 3, 5\}$, $C = \{3, 4\}$. Construya el diagrama en árbol de $A \times B \times C$ y luego, determine $A \times B \times C$.
12. Sea $|A| = 7$. Calcule $|A \times A|$. ¿Cuántas funciones $f : A \times A \to A$ hay?

13. Considere las operaciones binarias definidas por las siguientes funciones $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. Determine si f es conmutativa, asociativa o ambas.
    a. $f(x, y) = x + y - xy$.
    b. $f(x, y) = \text{máx}\{x, y\}$.
    c. $f(x, y) = x^y$
    d. $f(x, y) = x + y - 3$.
14. Sea A un conjunto y sea $f : A \times A \to A$ una operación binaria. Un elemento $e \in A$ se le llama **Identidad o Neutro** de f, si $f(a, e) = f(e, a) = a, \ \ \forall a \in A$. ¿Cuáles operaciones binarias tienen identidad en el ejercicio 2.?
15. Pruebe que si $f : A \times A \to A$ tiene identidad, esta es única.

16. Sean $f, g, h : \mathbb{Z} \to \mathbb{Z}$ definidas por $f(x) = x - 1, \;\; g(x) = 3x$ y

$$h(x) = \begin{cases} 0, & x \text{ par} \\ 1, & x \text{ impar} \end{cases}$$

Determine

a. $f \circ g, \;\; g \circ f, \;\; g \circ h, \;\; h \circ g, \;\; f \circ (g \circ h), \;\; (f \circ g) \circ h$

b. $f^2, \;\; f^3, \;\; g^2, \;\; g^3, \;\; h^2, \;\; h^3, \;\; h^{500}$

17. Sea U un conjunto universal y sean $S, T \subseteq U$. Sea $g : P(U) \to P(U)$ definida por $g(A) = T \cap (S \cup A)$ para $A \subseteq U$. Pruebe que $g^2 = g$.

18. Sea $g : \mathbb{N} \to \mathbb{N}$ definida por $g(n) = 2n$. Si $A = \{1, 2, 3, 4\}$ y $f : A \to \mathbb{N}$ definida por $f = \{(1, 2), (2, 3), (3, 5), (4, 7)\}$. Encuentre $g \circ f$.
19. Sean $f, g : \mathbb{R} \to \mathbb{R}$ definidas por $g(x) = 1 - x + x^2, \quad f(x) = ax + b$. Si $(g \circ f)(x) = 9x^2 - 9x + 3$, determine a y b.
20. Sean $f : A \to B$, $g : B \to C$. Pruebe que
    a. Si $g \circ f : A \to C$ es sobreyectiva, entonces g es sobreyectiva
    b. Si $g \circ f : A \to C$ es inyectiva, entonces f es inyectiva
21. Sean $A, B \subseteq U$ y $R_1, R_2 \subseteq A \times B$. Pruebe que
    a. $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$
    b. $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$
    c. $(R_1^{-1})^{-1} = R_1$

22. Determine si las funciones $f : \mathbb{R} \to \mathbb{R}$ siguientes tienen inversa o no. En caso afirmativo, encuentre f^{-1}.
    a. $f = \{(x, y)|2x + 3y = 7\}$.
    b. $f = \{(x, y)|y = x^3\}$.
    c. $f = \{(x, y)|ax + by = c,\ b \neq 0\}$.
    d. $f = \{(x, y)|y = x^4 - x\}$.
23. Sea $f : \mathbb{R} \to \mathbb{R}^+$ definida por $f(x) = e^{2x+5}$
    a. Halle la inversa f^{-1}
    b. Muestre que $f \circ f^{-1} = I_{\mathbb{R}^+}, \quad f^{-1} \circ f = I_{\mathbb{R}}$
    c. Represente f, f^{-1} en el mismo par de ejes de una gráfica
24. Encuentre f^{-1}, para las funciones siguientes:
    a. $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = -x$
    b. $f : \mathbb{R}^2 \to \mathbb{R}^2$ definida por $f(x, y) = (y, x)$

c. $f : \mathbb{R}^2 \to (\mathbb{R} \times \mathbb{R}^+)$ definida por $f(x, y) = (5x, e^y)$

25. Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2$. Determine $f^{-1}(B)$ si
    a. $B = \{0, 1\}$ b. $B = \{-1, 0, 1\}$. c. $B = [0, 1]$.
    d. $B = [0, 1)$. e. $B = [-1, 1]$ f. $B = [0, 4]$

26. Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = \operatorname{sen} x$. Encuentre $f^{-1}(B)$ si:

    a. $B = \{0\}$ b. $B = \{0, 1\}$ c. $B = [0, 1/2]$

Contenido

Introducción

En matemática el concepto de probabilidad es un número asociado a la ocurrencia o no de un evento o suceso. Este número indica qué tan frecuente puede ocurrir el suceso o evento. La probabilidad ofrece los procedimientos necesarios para analizar eventos que se producen al azar. En esta presentación nos enfocaremos al tratamiento de las probabilidades discretas, las cuales suelen estar relacionadas con la teoría de conteo. Suponga que una moneda no cargada, con lados C (cara) y E (escudo), se lanza al aire. La probabilidad o posibilidad de que el lado C quede hacia arriba es $1/2$. El 1 se debe a que sólo hay una posibilidad de C y el 2, al número total de posibilidades al lanzar la moneda. De la misma manera, suponga que lanza un dado, la

probabilidad de que salga un 3 en lado de arriba, es $1/6$. La probabilidad de que salga un número par es $3/6 = 1/2$, ya que hay tres posibilidades de números pares, que son los elementos del conjunto $\{2, 4, 6\}$.

Definiciones

Un **Experimento** es un proceso con el cual se obtiene un resultado. Un **Evento o suceso** es el resultado o combinación de resultados de un experimento. **Espacio muestral** es el conjunto de todos los resultados posibles al realizar un experimento. En el caso del lanzamiento de la moneda, el espacio muestral es $\{C, E\}$ y en el caso del lanzamiento del dado, el espacio muestral es $\{1, 2, 3, 4, 5, 6\}$.

Cuando los resultados de un espacio muestral finito tienen las mismas posibilidades de aparecer se dice que son equiprobables o igualmente probables y al espacio muestral se le llama **Espacio equiprobable**.
Los experimentos pueden ser **Deterministas o no deterministas (aleatorios)**. Un experimento es **Determinista** si se produce el mismo resultado cuando se realiza bajo las mismas condiciones. Es decir, se puede predecir el resultado. Un experimento es **No determinista (aleatorio)** si se puede producir resultados diferentes cuando se realiza bajo las mismas condiciones.
Es claro entonces que los espacios muestrales están asociados a experimentos aleatorios.

Sea $\Omega = \{e_1, e_2, \ldots, e_n, \ldots\}$ un espacio muestral. A los elementos e_k se les llama **Sucesos elementales** y a los subconjuntos de Ω

Sucesos. El conjunto potencia $P(\Omega)$ es el conjunto de todos los sucesos relacionados con un experimento aleatorio.
Al conjunto $\emptyset$ se le llama **Suceso imposible** y al espacio muestral Ω se le llama **Suceso seguro**.

Como un suceso es un conjunto, se pueden obtener nuevos sucesos mediante las operaciones entre conjuntos. Así, si A y B son sucesos, se tiene

a. $A \cup B$ es el suceso que se produce, si y sólo si ocurre A u ocurre B (o ambos).
b. $A \cap B$ es el suceso que se produce, si y sólo si ocurre A y ocurre B.
c. A^c es el suceso que ocurre, si y sólo si no ocurre A.

Definición

Dos sucesos A y B son **Mutuamente excluyentes o disjuntos o incompatibles** si no tienen elementos en común, es decir, si $A \cap B = \emptyset$.

Ejemplo

Sabemos que al lanzar un dado y observar la cara superior, se tiene un espacio muestral

$$\Omega = \{1, 2, 3, 4, 5, 6\}$$

Sea A el suceso en que sale un número par; B el suceso en que sale un número impar y D el suceso en que sale un número primo. Entonces

$$A = \{2, 4, 6\}, \qquad B = \{1, 3, 5\}, \qquad D = \{2, 3, 5\}.$$

Ahora podemos generar los sucesos

$$A \cup D = \{2, 3, 4, 5, 6\}, \qquad B \cap D = \{3, 5\}, \qquad D^c = \{1, 4, 6\},$$

donde $A \cup D$ es el suceso de salir un número par o un número primo
$B \cap D$ es el suceso en que sale un primo impar
D^c es el suceso en que no sale un número primo
Se observa que A y B son mutuamente excluyentes.

Definición

Sea A un suceso de un espacio muestral Ω. La **Probabilidad**, $Pr(A)$, del suceso A se define como

$$Pr(A) = \frac{|A|}{|\Omega|} = \frac{\text{Casos favorables}}{\text{Casos posibles}}.$$

Esta fórmula sólo es válida para un espacio equiprobable, es decir, cuando cada suceso elemental tiene la misma probabilidad. Por ejemplo, si el espacio muestral Ω tiene n puntos, la probabilidad de cada punto es $1/n$. De modo que si tenemos un suceso A de k puntos, la probabilidad $Pr(A) = k \,.\, \frac{1}{n} = \frac{k}{n}$.

Ejemplo

Suponga que se lanzan dos dados no cargados. ¿Cuál es la probabilidad de que la suma de los números en los dados sea 11?.

Solución

El espacio muestral está formado por los pares del producto cartesiano $\{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\}$ que tiene un cardinal de 36. De estos pares ordenados, los que suman 11 son: $(5, 6)$ y $(6, 5)$. Por tanto, la probabilidad es $2/36 = 1/18$.

Ejemplo

En una comunidad mayoritariamente femenina, hay un club de 100 miembros (85 mujeres y 15 hombres). Sea desea elegir al azar una

comisión de 5 miembros. ¿Cuál es la probabilidad de que la comisión esté formada solo por mujeres?.

Solución

Existen $C(100,5)$ maneras de elegir la comisión. Hay $C(85,5)$ maneras de seleccionar la comisión formada sólo por mujeres. Por tanto, la probabilidad de que la comisión esté formada por mujeres solamente es

$$\frac{C(85,5)}{C(100,5)} = \frac{85 \times 84 \times 83 \times 82 \times 81}{100 \times 99 \times 98 \times 97 \times 96} = 0.43568332.$$

Definición de probabilidad

Sea Ω un espacio muestral asociado a un experimento aleatorio y A un suceso. La **Probabilidad** se define como la aplicación

$$Pr : P(\Omega) \to [0, 1],$$

tal que

a. $Pr(A) \geq 0$

b. $Pr(\Omega) = 1$

c. Si $A_1, A_2, \ldots, A_n$ son sucesos mutuamente excluyentes dos a dos ($A_i \cap A_j = \emptyset, i \neq j$), entonces

$$Pr(\bigcup_{k=1}^{n} A_k) = \sum_{k=1}^{n} Pr(A_k).$$

Definición

Un **Espacio de probabilidad** es un par (Ω, Pr), donde Ω es un espacio muestral y Pr una aplicación de probabilidad definida sobre $P(\Omega)$.

Definición

Sea A un evento del espacio muestral Ω. La probabilidad de A se define como

$$Pr(A) = \sum_{a \in A} Pr(a).$$

Tomemos como ejemplo, el lanzamiento del dado que presentamos al inicio de la sección. La probabilidad de obtener un número par viene dada por

$$Pr(A) = Pr(\{2,4,6\}) = Pr(2) + Pr(4) + Pr(6) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}.$$

Teorema

Sean A, B y C eventos de un espacio muestral Ω. Entonces se verifican las propiedades siguientes:

a. $Pr(A^c) = 1 - Pr(A)$
b. $Pr(\emptyset) = 0$ (evento imposible)

c. $Pr(A - B) = Pr(A) - Pr(A \cap B)$. Si $A \subseteq B$, entonces $Pr(A) \leq Pr(B)$ y $Pr(B - A) = Pr(B) - Pr(A)$
d. $Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B)$
e. $Pr(A \cup B \cup C) = Pr(A) + Pr(B) + Pr(C) - Pr(A \cap B) - Pr(A \cap C) - Pr(B \cap C) + Pr(A \cap B \cap C)$

Demostración

a. Sabemos que $\Omega = A \cup A^c$. Entonces $Pr(\Omega) = Pr(A \cup A^c) = Pr(A) + Pr(A^c)$. De donde $1 = Pr(A) + Pr(A^c)$ y por tanto,

$$Pr(A^c) = 1 - Pr(A).$$

b. Sabemos que $\emptyset = \Omega^c$. Entonces $Pr(\emptyset) = Pr(\Omega^c) = 1 - Pr(\Omega) = 1 - 1 = 0$. Luego,

$$Pr(\emptyset) = 0.$$

c. Para probar la primera parte, descomponemos a A como $A = (A - B) \cup (A \cap B)$, donde $A - B$ y $A \cap B$ son disjuntos. De aquí que

$$Pr(A) = Pr(A - B) + Pr(A \cap B). \text{ Por tanto,}$$

$$Pr(A - B) = Pr(A) - Pr(A \cap B).$$

Para la segunda parte, procedemos de la siguiente manera: Como $A \subseteq B$, se tiene que $B = A \cup (B - A)$, donde A y $B - A$

son disjuntos. Entonces $Pr(B) = Pr(A) + Pr(B - A)$. De aquí, se obtiene que

$$Pr(A) \leq Pr(B) \text{ y } Pr(B - A) = Pr(B) - Pr(A).$$

d. Sabemos que $A \cup B = A \cup (B - A) = A \cup (B \cap A^c)$ y $B = B \cap (A \cup A^c) = (B \cap A) \cup (B \cap A^c)$. Los conjuntos que forman estas uniones son disjuntos. Entonces aplicando probabilidades se tiene

$$Pr(A \cup B) = Pr(A) + Pr(B \cap A^c) \text{ y}$$

$$Pr(B) = Pr(B \cap A) + Pr(B \cap A^c).$$

Si se resta miembro a miembro, se consigue que

$$Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B).$$

e. Para probar este resultado, se aplica el resultado del caso d repetidamente.

Ejemplo

Sean A y B dos sucesos aleatorios, tales que

$$Pr(A) = 3/8, \quad Pr(B) = 1/2, \quad Pr(A \cap B) = 1/4.$$

Encuentre

a. $Pr(A \cup B)$, $\quad Pr(A^c)$, $\quad Pr(B^c)$, $\quad Pr(A^c \cap B^c)$
b. $Pr(A^c \cup B^c)$, $\quad Pr(A \cap B^c)$, $\quad Pr(B \cap A^c)$

Solución

a. $Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B) = 3/8 + 1/2 - 1/4 = 5/8$

$Pr(A^c) = 1 - Pr(A) = 1 - 3/8 = 5/8$

$Pr(B^c) = 1 - Pr(B) = 1 - 1/2 = 1/2$

$Pr(A^c \cap B^c) = Pr((A \cup B)^c) = 1 - Pr(A \cup B) = 1 - 5/8 = 3/8$

b. $Pr(A^c \cup B^c) = Pr((A \cap B)^c) = 1 - Pr(A \cap B) = 1 - 1/4 = 3/4$

$Pr(A \cap B^c) = Pr(A - B) = Pr(A) - Pr(A \cap B) = 3/8 - 1/4 = 1/8$

$Pr(B \cap A^c) = Pr(B - A) = Pr(B) - Pr(B \cap A) = 1/2 - 1/4 = 1/4$

Ejemplo

Suponga que en una bolsa se tiene cuatro bolos de diferentes colores(blanco, negro, verde y rojo). Se sacan dos bolos de la bolsa.

a. ¿Cuál es el espacio muestral si el primer bolo se devuelve a la bolsa antes de sacar el segundo?.

$$\begin{aligned} \Omega &= \{BB, BN, BV, BR, NN, NB, NV, NR, VV, VB, \\ &\quad VN, VR, RR, RB, RV, RN\} \end{aligned}$$

b. ¿Cuál es el espacio muestral, si el primer bolo no se devuelve?.

$$\begin{aligned} \Omega &= \{BN, BV, BR, NB, NV, NR, VB, VN, \\ &\quad VR, RB, RV, RN\} \end{aligned}$$

Ejemplo

Suponga que una bolsa contiene 10 bolos blancos, 6 bolos negros y 8 bolos rojos. Se saca al azar un bolo. Calcular la probabilidad de

a. Sacar un bolo blanco.

$$Pr(\text{blanco}) = \frac{10}{24} = \frac{5}{12}$$

b. Sacar un bolo rojo.

$$Pr(\text{rojo}) = \frac{8}{24} = \frac{1}{3}$$

c. Sacar un bolo que no sea rojo.

$$Pr(\text{no rojo}) = 1 - Pr(\text{rojo}) = 1 - \frac{8}{24} = 1 - \frac{1}{3} = \frac{2}{3}$$

Ejemplo

Suponga que se saca una baraja al azar de un juego de 52 barajas. Sean los sucesos

$$A = \{x \,|\, x \text{ es un diamante}\}, \qquad B = \{x \,|\, x = \text{J, Q, K}\}.$$

Determine $Pr(A)$, $Pr(B)$, $Pr(A \cap B)$.

Solución

$$Pr(A) = \frac{\text{cantidad de diamantes}}{\text{cantidad de cartas}} = \frac{13}{52} = \frac{1}{4}.$$

$$Pr(B) = \frac{\text{cantidad de J, Q, K}}{\text{cantidad de cartas}} = \frac{12}{52} = \frac{3}{13}.$$

$$Pr(A \cap B) = \frac{\text{cantidad de diamantes que son J, Q, K}}{\text{cantidad de cartas}} = \frac{3}{52}.$$

Ejemplo

Suponga que se sacan 3 artículos al azar de una caja que contiene 15 artículos, de los cuales 5 son defectuosos. Suponga que

A es el suceso en que los tres artículos son defectuosos.

B es el suceso en que los tres artículos no son defectuosos.

Determine $Pr(A), \quad Pr(B)$.

Solución

El espacio muestral viene dado por $\Omega = \binom{15}{3} = 455$ maneras de escoger 3 artículos de 15.

El suceso A ocurre de $\binom{5}{3} = 10$ maneras de escoger 3 artículos defectuosos a partir de los 5 defectuosos.

El suceso B ocurre de $\binom{10}{3} = 120$ maneras de escoger 3 artículos no defectuosos a partir de 10 artículos no defectuosos.

$$Pr(A) = \frac{10}{455} = \frac{2}{91}.$$

$$Pr(B) = \frac{120}{455} = \frac{24}{91}.$$

Ejemplo

En unas elecciones se presentan dos candidatos (A, B) y una encuestadora selecciona una muestra de 200 personas para preguntar por cuál candidato van a votar. ¿cómo definir el espacio muestral?.

Solución

$$\Omega = \{(e_1, e_2, \cdots, e_{200}) \,|\, e_i \in \{A, B\}, i = 1, 2, \cdots, 200\}.$$

Ejemplo

Suponga que un dado se lanza 4 veces en forma consecutiva. ¿cuál es el espacio muestral?.

Solución

Suponga que $e_i,\ i = 1, 2, 3, 4$ es el resultado de lanzar el dado la i-ésima vez. Entonces

$$\Omega = \{(e_1, e_2, e_3, e_4) \,|\, e_i \in \{1, 2, 3, 4, 5, 6\},\ i = 1, 2, 3, 4\}.$$

Ejemplo

Suponga que se lanzan 4 dados simultaneamente. ¿Cómo se define el espacio muestral?.

Solución

Suponga que $e_i,\ i = 1, 2, 3, 4, 5, 6$ es la cantidad de veces que sale el número i en cada lanzamiento. Entonces un posible espacio muestral es

$$\Omega = \{(e_1, e_2, e_3, e_4, e_5, e_6) \,|\, e_i \in \{0, 1, 2, 3, 4\},\ \sum_{i=1}^{6} e_i = 4\}.$$

1. Sean A y B dos sucesos. Haga el diagrama de Venn y exprese simbólicamente los sucesos siguientes:
   a. A ocurre pero no B (sólo A).
   b. A o B, pero no ambos.
2. Sean A, B y C tres sucesos. Haga el diagrama de Venn y exprese simbólicamente los sucesos siguientes:
   a. Ocurren los sucesos A y B, pero no C.
   b. Sólo ocurre el suceso A.
3. Suponga que se lanza una moneda y un dado. El espacio muestral viene dado por

$$\Omega = \{C1, C2, C3, C4, C5, C6, E1, E2, E3, E4, E5, E6\}$$

   Exprese los siguientes sucesos en forma conjuntista:

a. El suceso A en que sólo aparecen caras y un número par.
b. El suceso B en que aparece un número primo.
c. El suceso c en que aparecen escudos y un número impar.
d. El suceso en que ocurren A o B.
e. El suceso en que ocurren B y C.
f. El suceso en que sólo ocurre B
g. ¿Cuáles sucesos son mutuamente excluyentes?.

4. Sea $\Omega = \{e_1, e_2, e_3, e_4\}$ un espacio muestral. Si es posible, ¿qué funciones define un espacio de probabilidad en Ω.

a. $Pr(e_1) = 1/2, \quad Pr(e_2) = 1/3, \quad Pr(e_3) = 1/4, \quad Pr(e_4) = 1/5.$
b. $Pr(e_1) = 1/2, \quad Pr(e_2) = 1/4, \quad Pr(e_3) = -1/4, \quad Pr(e_4) = 1/2.$
c. $Pr(e_1) = 1/2, \quad Pr(e_2) = 1/4, \quad Pr(e_3) = 1/8, \quad Pr(e_4) = 1/8.$
d. $Pr(e_1) = 1/2, \quad Pr(e_2) = 1/4, \quad Pr(e_3) = 1/4, \quad Pr(e_4) = 0.$

5. Sea $\Omega = \{e_1, e_2, e_3, e_4\}$ un espacio muestral y Pr una función de probabilidad en Ω.
   a. Encuentre $Pr(e_2)$, si $Pr(e_1) = 1/2, \quad Pr(e_3) = 1/6, \quad Pr(e_4) = 1/9$
   b. Encuentre $Pr(e_1)$ y $Pr(e_2)$, si $Pr(e_3) = Pr(e_4) = 1/4$, y $Pr(e_1) = 2Pr(e_2)$
   c. Encuentre $Pr(e_1)$, si $Pr(\{e_2, e_3\}) = 2/3$, $Pr(\{e_2, e_4\}) = 1/2$ y $Pr(e_2) = 1/8$
6. Suponga que una moneda cargada es lanzada, de modo que la posibilidad de que aparezca una cara es el doble de la que aparezca un escudo. Encuentre Pr(escudo) y Pr(cara).
7. Determine la probabilidad de cada suceso.
   a. que salga un número impar al lanzar un dado normal.
   b. que resulte un rey al sacar una sola baraja de un juego común de 52 barajas.

c. que salga por lo menos un escudo al lanzar tres monedas normales.
d. que aparezca una bola blanca al sacar una sola bola de una caja que contiene 5 bolas blancas, 4 bolas rojas y 3 bolas azules.

8. Suponga que se sacan al azar 2 cartas de una baraja común de 52 cartas. Encuentre la probabilidad de que:
   a. ambas sean diamantes.
   b. una sea diamante y la otra sea un corazón
9. Suponga que se escogen tres bombillos al azar de 15, de los cuales 5 están defectuosos. Encuentre la probabilidad de que:
   a. ninguno esté defectuoso.
   b. exactamente uno esté defectuoso.
   c. por lo menos uno esté defectuoso.

10. Suponga que se seleccionan al azar 2 cartas numeradas de 1 a 10. Encuentre la probabilidad de que la suma sea impar si:
    a. las 2 cartas se sacan juntas.
    b. se saca una, después la otra, sin reposición.
    c. las 2 cartas se sacan una después de la otra con reposición.

Contenido

Consideremos un suceso B de un espacio muestral Ω, con $Pr(B) > 0$. La probabilidad de que ocurra un suceso A dado que ha ocurrido B o sea la **probabilidad condicional** de A dado que ha sucedido B se define como

$$Pr(A \mid B) = \frac{Pr(A \cap B)}{Pr(B)}.$$

Si Ω es un espacio equiprobable, se tiene que

$$Pr(A \cap B) = \frac{|A \cap B|}{|\Omega|}, \qquad Pr(B) = \frac{|B|}{|\Omega|}.$$

De modo que

$$Pr(A \mid B) = \frac{Pr(A \cap B)}{Pr(B)} = \frac{|A \cap B|}{|\Omega|}.$$

Ejemplo

Sean A y B dos sucesos aleatorios tales que
$Pr(A) = 1/4, \qquad Pr(B) = 1/3, \qquad Pr(A \cap B) = 1/5$. Entonces

$$Pr(A \mid B) = \frac{Pr(A \cap B)}{Pr(B)} = \frac{1/5}{1/3} = 3/5$$

$$Pr(B \mid A) = \frac{Pr(B \cap A)}{Pr(A)} = \frac{1/5}{1/4} = 4/5$$

$$\begin{aligned} Pr(A \cup B) &= Pr(A) + Pr(B) - Pr(A \cap B) \\ &= 1/4 + 1/3 - 1/5 = 23/60 \end{aligned}$$

$$
\begin{aligned}
Pr(A^c \mid B) &= \frac{Pr(A^c \cap B)}{Pr(B)} = \frac{Pr(B) - Pr(A \cap B)}{Pr(B)} \\
&= \frac{1/3 - 1/5}{1/3} = 2/5
\end{aligned}
$$

$$
\begin{aligned}
Pr(B^c \mid A^c) &= \frac{Pr(B^c \cap A^c)}{Pr(A^c)} = \frac{Pr((A \cup B)^c)}{1 - Pr(A)} \\
&= \frac{1 - Pr(A \cup B)}{1 - Pr(A)} = \frac{1 - 23/60}{1 - 1/4} \\
&= \frac{37/60}{3/4} = 37/45
\end{aligned}
$$

$$\begin{aligned} Pr(B^c \mid A) &= \frac{Pr(B^c \cap A)}{Pr(A)} = \frac{Pr(A) - Pr(A \cap B)}{Pr(A)} \\ &= \frac{1/4 - 1/5}{1/4} = 1/5 \end{aligned}$$

Ejemplo

Suponga que una fábrica produce tres tipos de artículos (A, B, C) en dos turnos de trabajo (turno 1 y turno 2). En el turno 1 se produce 5 del tipo A, 4 del tipo B y 8 del tipo C y en el turno 2, se produce 7 del tipo A, 3 del tipo B y 5 del tipo C. Si tabulamos estos datos se tiene:

Turnos \ Tipos	tipo A	tipo B	tipo C	Total
turno 1	5	4	8	17
turno 2	7	3	5	15
Total	12	7	13	32

a. Cuál es el porcentaje de los artículos producidos en el turno 2?.

$$Pr(\text{turno 2}) = \frac{15}{32} = 0.47 = 47\,\%$$

b. Cuál es el porcentaje de producción de artículos del tipo B?.

$$Pr(\text{tipo B}) = \frac{7}{32} = 0.22 = 22\,\%$$

c. Cuál es la probabilidad de que un artículo del tipo A se produzca en el turno 1?.

$$Pr(\text{turno 1} \mid \text{tipo A}) = \frac{5}{12} = 0.42$$

Ejemplo

Suponga que una clase de informática tiene 20 alumnos (10 varones y 10 hembras). De estos alumnos, 5 varones y 5 hembras escogieron lenguajes formales como materia optativa.

a. ¿Cuál es la probabilidad de que un alumno elegido al azar sea varon o estudie lenguajes formales?

$$Pr(\text{varón o lenguajes formales}) = \frac{15}{20} = 0.75$$

b. ¿Cuál es la probabilidad de que un alumno(a) elegido(a) al azar sea hembra y no estudie lenguajes formales?

$$Pr(\text{hembra y no lenguajes formales}) = \frac{5}{20} = 0.25$$

Ejemplo

Suponga que se lanzan dos dados. Si la suma de los dos dados es 6, hallar la probabilidad de que uno de los números sea un 2.

Solución

En este caso, tomemos el suceso $B = \{(1,5),(2,4),(3,3),(4,2),(5,1)\}$ y el suceso $A = \{(x,y) \,|\, x = 2 \text{ o } y = 2\} = \{(2,4),(4,2)\}$. Debemos encontrar

$$Pr(A \mid B) = \frac{Pr(A \cap B)}{Pr(B)} = \frac{|A \cap B|}{|B|} = \frac{2}{5}.$$

Definición

Una sucesión finita de experimentos donde cada experimento tiene un número finito de resultados con sus probabilidades se le llama **Proceso estocástico finito.** Normalmente se utiliza un diagrama de árbol para describir un proceso estocástico.

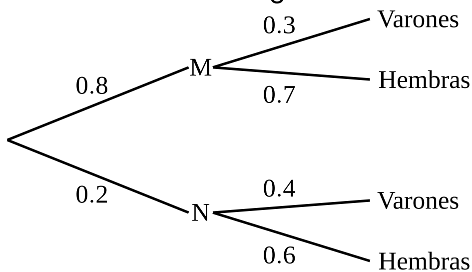
Ejemplo

En un Liceo los estudiantes se deciden por hacer el cuarto de matemática o el cuarto de naturales. En un determinado año, el 80 % se decide por matemática y el resto por naturales. EL 30 % de los que

se deciden por matemática son varones y el 40 % de los que se deciden por naturales son varones. Suponga que se elige al azar un estudiante. ¿Cuál es la probabilidad de que sea hembra?.

Solución

Consideremos el diagrama de árbol siguiente:



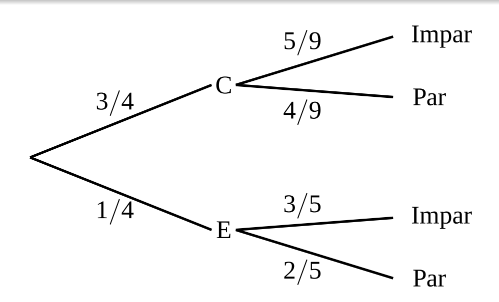
$Pr(\text{hembra}) = 0.8 * 0.7 + 0.2 * 0.6 = 0.68$.

Ejemplo

Suponga que se lanza una moneda cargada, tal que $Pr(\text{cara}) = 3/4$ y $Pr(\text{escudo}) = 1/4$. Si sale cara, se selecciona al azar un número del 1 al 9. Si sale escudo, se selecciona al azar un número del 1 al 5. ¿Cuál es la probabilidad de seleccionar un número par?.

Solución

Observemos el diagrama de árbol siguiente:


5/9
Impar
3/4
C
Par
4/9
3/5
1/4
Impar
E
2/5
Par

$Pr(\text{par}) = 3/4 * 4/9 + 1/4 * 2/5 = 13/30.$

Si A, B y C son tres sucesos, se puede probar que

$$Pr(A \cap B \cap C) = Pr(A)Pr(B \mid A)Pr(C \mid A \cap B).$$

En general se tiene el **Principio de la multiplicación para probabilidad condicional**

Sean $A_1, A_2, A_3, \cdots, A_n$ sucesos. Entonces

$$\begin{aligned} Pr(A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n) \quad = \quad & Pr(A_1)Pr(A_2 \mid A_1) \\ & Pr(A_3 \mid A_1 \cap A_2) \\ & Pr(A_4 \mid A_1 \cap A_2 \cap A_3) \cdots \\ & Pr(A_n \mid A_1 \cap A_2 \cap \cdots \cap A_{n-1}) \end{aligned}$$

Ejemplo

Suponga que una funda contiene 9 bolas azules y 3 bolas rojas. Si se seleccionan al azar 3 bolas, ¿cuál es la probabilidad de que todas las bolas sean azules?.

Solución

La probabilidad de que la primera bola seleccionada sea azul es de $9/12$. Si la primera bola seleccionada es azul, la probabilidad de que la segunda sea azul es de $8/11$, dado que sólo quedan 8 bolas azules de 11 bolas. De la misma manera, si las primeras dos bolas seleccionadas son azules, la probabilidad de que la tercera bola sea azul es de $7/10$, dado que quedan 7 bolas azules de 10 bolas. Luego,

según el principio de la multiplicación, la probabilidad de que las tres bolas seleccionadas sean azules es de

$$Pr(\text{tres bolas azules}) = \frac{9}{12} \cdot \frac{8}{11} \cdot \frac{7}{10} = \frac{21}{55}.$$

Definición

Se dice que los sucesos A y B son **Independientes** si la probabilidad de que el suceso A ocurra no está influenciada por el hecho de que el suceso B haya o no ocurrido. Es decir, si la probabilidad de A es igual a la probabilidad condicional de A dado B ($Pr(A) = Pr(A \mid B)$). En otras palabras, si

$$Pr(A \cap B) = Pr(A)\, Pr(B).$$

En caso contrario, se dice que los sucesos son dependientes.

Ejemplo

Suponga que se lanzan dos dados: uno azul y uno rojo. Se observa los números que salen en la cara superior. Sea A el suceso “la suma de los dados es igual a 7” y B el suceso “ el dado rojo es par ”. ¿Son los sucesos A y B independientes?.

Solución

El suceso $A = \{(1,6),(2,5),(3,4),(4,3),(5,2),(6,1)\}$. Entonces $Pr(A) = \dfrac{6}{36} = \dfrac{1}{6}$.

EL suceso $B = \{(x,y)\,|\,x =$ es un número del dado azul, $\;y = 2,4,6\}$. Entonces $Pr(B) = \dfrac{18}{36} = \dfrac{1}{2}$. (Observe que por cada número del dado azul hay 3 números pares del dado rojo).

$A \cap B = \{(5,2),(3,4),(1,6)\}$ Entonces $Pr(A \cap B) = \dfrac{3}{36} = \dfrac{1}{12}$.

Luego, $Pr(A \cap B) = Pr(A)Pr(B) = \dfrac{1}{6} \cdot \dfrac{1}{2} = \dfrac{1}{12}$ y por tanto, los sucesos son independientes.

Ejemplo

Suponga que la probabilidad de que el disparo, representando el suceso A de en el blanco es $\frac{1}{2}$ y la probabilidad de que el disparo, representando al suceso B de en el blanco es $\frac{2}{3}$. ¿Cuál es la probabilidad de que el blanco sea alcanzado si tanto A como B disparan al blanco?.

Solución

Se tiene que $Pr(A) = \frac{1}{2}, \qquad Pr(B) = \frac{2}{3}$. Es claro que el suceso A no tiene infuencia en el suceso B ni el suceso B en el A , por lo que son independientes. Es decir que $Pr(A \cap B) = Pr(A)Pr(B) = \frac{1}{2} . \frac{2}{3} = \frac{1}{3}$.

Ahora, tenemos

$$Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B) = \frac{1}{2} + \frac{2}{3} - \frac{1}{3} = \frac{5}{6}.$$

Definición

Los sucesos A, B y C son **independientes** si se satisfacen las condiciones siguientes:

a. $Pr(A \cap B) = Pr(A)Pr(B), \quad Pr(A \cap C) = Pr(A)Pr(C), \quad Pr(B \cap C) = Pr(B)Pr(C)$

b. $Pr(A \cap B \cap C) = Pr(A)Pr(B)Pr(C)$

Ejemplo

Suponga que la probabilidad de que Juan viaje a la Vega es de $\frac{3}{5}$ y la probabilidad de que llueva en San Pedro es de $\frac{4}{5}$. ¿Cuál es la probabilidad de que Juan viaje a la Vega y llueva en San Pedro?.

Solución

Es claro que estos sucesos son independientes, por lo que

$$Pr(A \cap B) = Pr(A)Pr(B) = \frac{3}{5} \cdot \frac{4}{5} = \frac{12}{25}.$$

1. Sean A y B dos sucesos aleatorios tales que
   $Pr(A) = 1/2, \quad Pr(B) = 1/3, \quad Pr(A \cap B) = 1/4$. Encuentre
   a. $Pr(A \mid B), \qquad Pr(B \mid A)$
   b. $Pr(A \cup B), \qquad Pr(A^c \mid B^c)$
   c. $Pr(A^c \cap B^c), \qquad Pr(B^c \mid A^c)$
2. Suponga que se lanzan dos dados. Encuentre la probabilidad de que la suma sea 10 o mayor, si:
   a. sale un 5 en el primer dado.
   b. sale un 5 en por lo menos, uno de los dos dados.
3. Suponga que se lanzan 3 monedas. Encuentre la probabilidad de que todas salgan caras, si:
   a. la primera moneda resulta cara.
   b. una de las monedas resulta cara.

4. Suponga que lanzan dos dados. Si los dos números que aparecen son diferentes, encuentre la probabilidad de que:
   a. la suma sea seis.
   b. aparezca un uno.
   c. la suma sea 4 o menos.
5. Se escogen dos dígitos al azar del 1 al 9. Si la suma es par, encuentre la probabilidad de que ambos números sean impares.
6. En una Universidad, el 25 % de los estudiantes quemó matemática, el 15 % quemó química, y el 10 % quemó tanto matemática como química. Se selecciona un estudiante al azar.
   a. Si quemó química, ¿cuál es la probabilidad de que haya quemado matemática?.
   b. Si quemó matemática, ¿cuál es la probabilidad de que haya quemado química?.

c. ¿Cuál es la probabilidad de que haya quemado matemática o química?.

7. Sean A y B dos sucesos, tales que $Pr(A) = 3/8, \quad Pr(B) = 5/8, Pr(A \cup B) = 3/4$. Encuentre $Pr(A \,|\, B)$ y $Pr(B \,|\, A)$.
8. Sea $\Omega = \{1, 2, 3, 4, 5\}$, tal que $Pr(1) = Pr(2) = 1/10$, $Pr(3) = 1/5$, $Pr(4) = Pr(5) = 3/16$ y sea $A = \{1, 2, 3\}, \;\; B = \{3, 4, 5\}, \;\; C = \{1, 3, 5\}, \;\; D = \{1, 5\}, \;\; E = \{2, 3, 4\}$. Encuentre

   a. $Pr(A \,|\, E), \qquad Pr(A \,|\, E)$

   b. $Pr(C \,|\, E), \qquad Pr(D \,|\, E)$
9. Se extraen tres cartas de una baraja común de 52 cartas.

   a. ¿Cuál es la probabilidad que salgan 3 As, si es con reemplazamiento?

b. ¿Cuál es la probabilidad que salgan 3 As, si es sin reemplazamiento?

10. Sean A, B y C tres sucesos independientes. Si $Pr(A) = 0.5, \quad Pr(B) = 0.1, \quad Pr(C) = 0.7$ Encuentre las probabilidades de los sucesos $A \cap (B^c \cup C)$ y $A \cup ((B \cup C)^c)$

11. Una fábrica produce el 50 % de los artículos de tipo A, el 30 % de los artículos de tipo B y el 20 % de los artículos de tipo C que se producen en el país. El porcentaje de los artículos defectuosos es de 3 %, 4 % y 5 % respectivamente. Si se selecciona un artículo al azar.
    a. Desarrolle un diagrama de árbol.
    b. ¿Cuál es la probabilidad de que el artículo esté defectuoso?.
    c. ¿Cuál es la probabilidad de que el artículo no esté defectuoso?

12. Suponga que una urna contiene tres monedas. una común (cara y escudo), otra tiene dos caras y la tercera está cargada, de modo que la probabilidad de obtener cara es de $\frac{1}{3}$. Se saca una moneda y se lanza. Entonces
    a. Haga un diagrama de árbol.
    b. ¿Cuál es la probabilidad de obtener cara?.
13. Encuentre $Pr(B \mid A)$ si:
    a. A es un subconjunto de B
    b. A y B son mutuamente excluyentes.

13. Suponga que A y B son dos cajas que contienen: 3 bolas rojas y 2 bolas blancas la caja A y 2 bolas rojas y 5 bolas blancas la caja B. Se selecciona una de las cajas al azar; se toma una bola y se coloca en la otra caja; luego, se saca una bola de la segunda caja. ¿Cuál es la probabilidad de que ambas bolas sacadas sean del mismo color?. Construya el diagrama de árbol.
14. Sea A el suceso en que un programador conoce dos lenguajes de programación (Java y C++) y sea B el suceso en que un programador conoce por menos C++.
    a. Demostrar que A y B son sucesos independientes, si un programador conoce tres lenguanjes de programación.
    b. Demostrar que A y B son sucesos dependientes, si un programador conoce dos lenguanjes de programación.

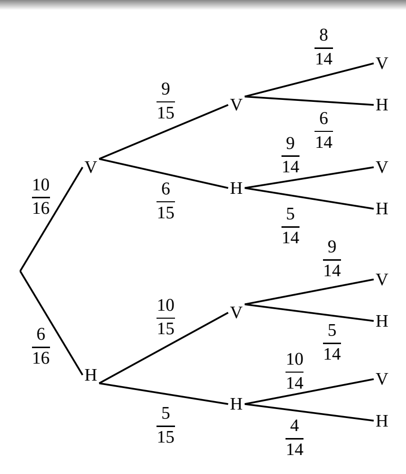
Ejercicios

15. Demuestre que si A y B son sucesos independientes, entonces A^c y B^c son sucesos independientes.
16. Demuestre que si A y B son sucesos independientes, entonces A y B^c son sucesos independientes.
17. Sean A y B sucesos tales que
$Pr(A) = 1/4, \quad Pr(A \cup B) = 1/3, \quad Pr(B) = p$.
    a. Encuentre p, si A y B son mutuamente excluyentes.
    b. Encuentre p, si A y B son independientes.
    c. Encuentre p, si A es un subconjunto de B.
18. Sean A y B sucesos independientes, tales que $Pr(A) = 1/2$ y $Pr(A \cup B) = 2/3$. Encuentre
    a. $Pr(B)$.
    b. $Pr(A \,|\, B)$.

   c. $Pr(B^c \mid A)$.

19. Demuestre mediante un contraejemplo que si A, B y C son sucesos independientes dos a dos, no implica que sean independientes.
20. Demuestre que si A, B y C son sucesos independientes, entonces $A \cup B$ y C son independientes.
21. Demuestre que un suceso A es independiente de si mismo si y sólo si su probabilidad es 0 o 1.
22. Suponga que una sección de informática consta de 10 estudiantes varones y 6 estudiantes hembras. Si se escoge un comité de tres al azar, Considere el siguiente diagrama de árbol para calcular:
    a. la probabilidad de seleccionar tres varones.

b. la probabilidad de seleccionar exactamente dos varones y una hembra.
c. la probabilidad de seleccionar por lo menos un varón.
d. la probabilidad de seleccionar exactamente dos hembras y un varón.


V
H
10/16
6/16
V
H
9/15
6/15
V
H
10/15
5/15
V
H
8/14
6/14
V
H
9/14
5/14
V
H
9/14
5/14
V
H
10/14
4/14

Contenido

Las variables aleatorias representan el mecanismo fundamental para modelar fenómenos aleatorios o estocásticos. Producen valores reales casi siempre, ligados a resultados de un experimento aleatorio. El número de caras que se observan al lanzar 10 monedas no cargadas; la suma de los números que quedan en la cara superior al lanzar dos dados, son ejemplos de variables aleatorias.
Las variables aleatorias se clasifican según el tipo de datos que producen en : discretas, continuas y mixtas, las cuales a su vez pueden ser : unidimensionales, bidimensionales, tridimensionales, etc., dependiendo de la cantidad de características que se estudie.
Parece ser que el nombre de variable aleatoria produce uno de los errores de nombre más desafortunados que se han dado en toda la matemática, puesto que una variable aleatoria es una función definida

en un espacio muestral y no una variable. Esta terminología es un estándar en la literatura científica, por lo que se hace prácticamnete imposible deshacerse de ella. De manera que nosotros también seguiremos con ella en este pequeño estudio.

Definición

Sea (Ω, Pr) un espacio de probabilidad. Una variable aleatoria se define como una función

$$X : \Omega \to W \quad \text{(generalmente } \mathbb{R}\text{)}$$

Ejemplo

Suponga que se lanza dos monedas. El espacio muestral asociado a este experimento es

$$\Omega = \{CC, CE, EC, EE\}.$$

Suponga que la variable aleatoria X, es el número de caras que se observa en el lanzamiento. Entonces

$$X(CC) = 2, \;\; X(CE) = X(EC) = 1, \;\; X(EE) = 0.$$

Definición

El conjunto

$$W_X = \{w \in W \mid \exists e \in \omega, X(e) = w\}$$

se le llama **Recorrido o rango** de la variable aleatoria y se puede decir que representa otro espacio muestral. El recorrido del ejemplo anterior es

$$W_X = \{0, 1, 2\}.$$

Ejemplo

Si suponemos que las monedas del ejemplo anterior no están cargada, tenemos que

$$Pr(CC) = \frac{1}{4}, \ \ Pr(CE) = \frac{1}{4}, \ \ Pr(EC) = \frac{1}{4}, \ \ Pr(EE) = \frac{1}{4}.$$

Ahora podemos escribir que

$$Pr(X = 1) = \frac{1}{2}, \;\; Pr(X = 2) = \frac{1}{4}, \;\; Pr(X = 0) = \frac{1}{4}.$$

Ejemplo

Sea Ω el espacio muestral asociado al lanzamiento de dos dados. Sea $X : \Omega \to \mathbb{N}$ la variable aleatoria que representa la suma de los números que se observan en las caras superiores. Así que,

$$X[(1,2)] = 3, \;\; X[(5,5)] = 10, \;\; X[(4,3)] = 7, \;\; X[(2,3)] = 5$$

son algunos ejemplos. Sea A el evento en que la suma sea 9. Entonces

$$A = \{(3,6),(4,5),(5,4),(6,3)\}.$$

Así que $Pr(A) = 4/36 = 1/9$. De manera que $Pr(X = 9) = 1/9$. En este caso se interpreta a "$X = 9$" como un evento. En lugar de "$X = 9$" también se puede escribir el conjunto

$$A = \{e \in \Omega \,|\, X(e) = 9\}.$$

Volviendo al ejemplo del lanzamiento de las dos monedas anterior. ¿ Cuál es la probabilidad de que $X \geq 1$?. Es decir, ¿Cuál es la $Pr(X \geq 1)$?.

Solución

Consideremos el evento $A = \{CC, CE, EC\}$, cuyos elementos hacen que la variable aleatoria X tome los valores de 1 0 2. Así que

$$Pr(A) = \frac{3}{4}. \text{ Luego, } Pr(X \geq 1) = \frac{3}{4}.$$

Definición

Función de distribución de una variable aleatoria es una función $F_X(x)$ que asigna a cada número real x la probabilidad de que la variable aleatoria tome valores menores o iguales a x. Es decir,

$$F_X(x) = Pr(X \leq x).$$

La función $F_X(x)$ debe satisfacer las siguientes condiciones:

a. $F_X(x)$ es monótona no decreciente. Es decir, si $x_1 \leq x_2$, entonces $F_X(x_1) \leq F_X(x_2)$.

b. $\lim\limits_{x \to -\infty} F_X(x) = 0$.

c. $\lim\limits_{x \to \infty} F_X(x) = 1$.

d. $F_X(x)$ es continua por la derecha. Es decir, $\lim\limits_{x \to x_0^+} = F_X(x_0)$.

Como se observa en la definición, la función de distribución es la probabilidad acumulada hasta el número x. A cada variable aleatoria le corresponde una función de distribución.

Ejemplo

La función de distribución para el experimento del lanzamiento de las dos monedas, donde la variable aleatoria es el número de caras es como sigue:

$$F_X(x) = Pr(X \leq x) = \begin{cases} 0, & \text{si } x < 0 \\ 1/4, & \text{si } 0 \leq x < 1 \\ 3/4, & \text{si } 1 \leq x < 2 \\ 1, & \text{si } x \geq 2 \end{cases}$$

La representación gráfica de la función de distribución es siempre escalonada.

Ejemplo

Suponga que se lanza un dado y sea X la variable aleatoria que representa el número que sale en la cara superior. Entonces

$$Pr(X = x_i) = 1/6, \quad x_i = i, i = 1, 2, 3, 4, 5, 6.$$

La función de distribución $F_X(x)$ se define como:

$$F_X(x) = Pr(X \leq x) = \begin{cases} 0, & \text{si} \;\; x < 1 \\ 1/6, & \text{si} \;\; 1 \leq x < 2 \\ 2/6, & \text{si} \;\; 2 \leq x < 3 \\ 3/6, & \text{si} \;\; 3 \leq x < 4 \\ 4/6, & \text{si} \;\; 4 \leq x < 5 \\ 5/6, & \text{si} \;\; 5 \leq x < 6 \\ 1, & \text{si} \;\; x \geq 6 \end{cases}$$

Ejemplo

Se puede comprobar que la función

$$F(x) = \frac{1}{1+e^{-x}}, \quad -\infty < x < \infty$$

representa una función de distribución. Basta con comprobar que se satisfacen las condiciones de la función de distribución.

Variable aleatoria discreta

Sea Ω un espacio muestral y $X : \Omega \to W$ una variable aleatoria. Si el recorrido de X, W_X, es finito o infinito numerable (un conjunto discreto) , se dice que X es una **Variable aleatoria discreta**. Por ejemplo, las variables aleatorias que hemos definido en los ejemplos anteriores son discretas. En otras palabras, una variable aleatoria es discreta si sólo toma valores enteros.

Definición

Sea X una variable aleatoria discreta (recorrido finito o infinito numerable) definida sobre un espacio muestral Ω. Se llama **Función de probabilidad o función de probabilidad puntual** de la variable aleatoria X a la función P que asigna a cada valor x_i de X su probabilidad ($P(x_i) = Pr(X = x_i)$). Esta función debe satisfacer las condiciones siguientes:

a. $P(x_i) \geq 0, \quad \forall i$

b. $\sum_{i=1}^{\infty} P(x_i) = 1$

A esta función también se le llama **Función de densidad discreta o función de cuantía**

Ejemplo

Sea X una variable aleatoria discreta, cuya función de densidad es

$$Pr(X = x) = \frac{x+1}{15}, \quad x = 0, 1, 2, 3, 4.$$

a. Probar que Pr es una función de densidad.

Es claro que $0 \leq Pr(X = x) \leq 1$. Además

$$\sum_{x=0}^{4} Pr(X = x) = \frac{1}{15} + \frac{2}{15} + \frac{3}{15} + \frac{4}{15} + \frac{5}{15} = 1.$$

Luego, es una función de densidad.

b. Encuentre $Pr(X \geq 3)$

$$Pr(X \geq 2) = \frac{3}{15} + \frac{4}{15} + \frac{5}{15} = \frac{12}{15} = \frac{4}{5}.$$

Definición

Una variable aleatoria X se dice **Continua** si existe una función f, llamada **Función de densidad de probabilidad** de X, que satisface las condiciones siguientes:

a. $f(x) \geq 0, \ \ \forall x$

b. $\displaystyle\int_{-\infty}^{+\infty} f(x)\,\mathrm{d}x = 1$

c. $\displaystyle Pr(a \leq X \leq b) = \int_a^b f(x)\,\mathrm{d}x, \ \ \forall a, b \ni -\infty < a < b < +\infty$

En otras palabras, una variable aleatoria X es continua si puede tomar todos los valores de un intervalo. Este intervalo puede ser $(-\infty, +\infty)$.

La estatura de los estudiantes de la clase de matemática discreta; la duración en horas de un bombillo eléctrico; el tiempo de funcionamiento de un equipo en estado de prueba, son ejemplos de una variable aleatoria continua.

Ejemplo

Sea X un variable aleatoria continua, cuya función de densidad de probabilidad viene dada por:

$$f(x) = \begin{cases} 2x, & 0 < x < 1 \\ 0, & \text{para cualquier otro valor} \end{cases}$$

Se observa claramente que $f(x)$ es ciertamente una función de densidad, puesto que:

a. $f(x) \geq 0$

b. $\int_{-\infty}^{+\infty} f(x)\,\mathrm{d}x = \int_0^1 2x\,\mathrm{d}x = 1$

Si queremos calcular $Pr(X \leq \frac{1}{2} \,\Big|\, \frac{1}{3} \leq X \leq \frac{2}{3})$, podemos aplicar el concepto de probabilidad condicional y decir que

$$
\begin{aligned}
Pr(X \leq \frac{1}{2} \,\Big|\, \frac{1}{3} \leq X \leq \frac{2}{3}) &= \frac{Pr(\frac{1}{3} \leq X \leq \frac{1}{2})}{Pr(\frac{1}{3} \leq X \leq \frac{2}{3})} \\
&= \frac{\int_{1/3}^{1/2} 2x \, \mathrm{d}x}{\int_{1/3}^{2/3} 2x \, \mathrm{d}x} = \frac{5/36}{1/3} = \frac{5}{12}
\end{aligned}
$$

En el caso de las variables aleatorias continuas, la función de distribución se define como:

$$F_X(x) = Pr(X \leq x) = \int_{-\infty}^{x} f(s) \, \mathrm{d}s.$$

De aquí y por el teorema fundamental del cálculo se tiene

$$\frac{\mathrm{d}}{\mathrm{d}x} F_X(x) = f(x).$$

Las variables aleatorias continuas tienen la condición de que la probabilidad de un punto es siempre cero. Es decir que

$$Pr(X = x) = 0.$$

De modo que:

$$\begin{aligned} Pr(a \leq X \leq b) &= Pr(a < X \leq b) \\ &= Pr(a \leq X < b) \\ &= Pr(a < X < b). \end{aligned}$$

Atendendiendo a las definiciones de las variables aleatorias continuas, función de densidad y función de distribución, se tiene las fómulas siguientes:

a. $Pr(a < X \leq b) = F_X(b) - F_X(a) = \int_a^b f(x)\,\mathrm{d}x$

b. $Pr(X > a) = 1 - Pr(X \leq a) = 1 - F_X(a) = \int_a^\infty f(x)\,\mathrm{d}x$

c. $Pr(X \leq b) = F_X(b) = \int_{-\infty}^b f(x)\,\mathrm{d}x = 1 - \int_b^\infty f(x)\,\mathrm{d}x$

Ejemplo

Sea X una variable aleatoria continua, cuya función de distribución es:

$$F_X(x) = \frac{1}{1+e^{-x}}, \quad -\infty < x < \infty.$$

Entonces su función de densidad es:

$$f(x) = \frac{\mathrm{d}}{\mathrm{d}x} F_X(x) = \frac{e^{-x}}{(1+e^{-x})^2}, \quad -\infty < x < \infty.$$

Ejemplo

Sea X una variable aleatoria continua, cuya función de distribución se define como:

$$F_X(x) = \begin{cases} 0, & x \leq 0 \\ 1 - e^{-x}, & x > 0 \end{cases}$$

Entonces

$$F'_X(x) = f(x) = \begin{cases} e^{-x}, & x \geq 0 \\ 0, & \text{para cualquier otro valor} \end{cases}$$

Variables aleatorias mixtas

Aunque hay casos en que aparecen las variables aleatorias mixtas, no son los más frecuentes en las aplicaciones. Las variables aleatorias

discretas y continuas son realmente las más importantes en el estudio de las aplicaciones. Las situaciones en que aparecen las variables aleatorias mixtas se producen como una combinación de las variables discretas y continuas y están fuera del alcance de este material.

1. Suponga que se lanza un par de dados. Sea X la variable aleatoria "suma de los números obtenidos". Encuentre la función de probabilidad.
2. Sea X una variable aleatoria discreta, cuya función de probabilidad viene dada por:

x_i	0	1	2	3	4	5
$Pr(X = x_i)$	0.1	0.2	0.1	0.4	0.1	0.1

   a. Calcule y grafique la función de distribución.
   b. Calcule $Pr(X < 4.5)$, $Pr(X \geq 3)$, $Pr(3 \leq X < 4.5)$
3. Suponga que lanza una moneda 3 veces. Sea X la variable aleatoria que representa en número de caras.
   a. Encuentre el espacio muestral Ω.

b. ¿Cuáles son los posibles valores de X.
c. Encuentre la función de probabilidad de X.
d. ¿Cuál es la probabilidad de que salga al menos dos caras?.
e. ¿Cuál es la probabilidad de que el número de caras esté entre 1 y 2?.

4. Sea X una variable aleatoria continua, cuya función de densidad se define como:

$$f(x) = \begin{cases} 42x(1-x)^5, & 0 < x \leq 1 \\ 0, & \text{para otros valores} \end{cases}$$

Encuentre la función de distribución $F_X(x)$.

5. Suponga que la variable aleatoria X tiene la función de probabilidad siguiente:

x_i	1	2	3	4	5
$Pr(X = x_i)$	0.05	0.20	0.05	0.45	0.25

   a. Compruebe que es una función de probabilidad.
   b. Calcule $Pr(X \leq 3)$.
   c. Calcule $Pr(X > 3)$.
   d. Calcule $Pr(X = 1 \text{ o } X = 3 \text{ o } X = 5)$.
   e. Represente la función de distribución $F_X(x)$.

6. Sea X una variable aleatoria continua, cuya función de densidad de probabilidad se define como:

$$f(x) = \begin{cases} k(1+x^2), & 0 < x < 3 \\ 0, & \text{para otros valores} \end{cases}$$

   a. Encuentre k y la función de distribución $F_X(x)$.
   b. Calcule $Pr(1 < X < 2)$.
   c. Calcule $Pr(X < 1)$.
   d. Calcule $Pr(X < 2 \,|\, X > 1)$.

7. Sea X una variable aleatoria continua, cuya función de distribución se define como:

$$F_X(x) = \begin{cases} 0, & x < -2 \\ 0.4, & -2 \leq x < 0.5 \\ 0.8, & 0.5 \leq x < 3 \\ 1, & x \geq 3 \end{cases}$$

   a. Represente gráficamente a $F_X(x)$.
   b. Calcule la función de probabilidad de X.

8. Sea X una variable aleatoria, cuya función de probabilidad se define como:

$$P(X = k) = \begin{cases} \frac{3}{2}\frac{1}{k!(4-k)!}, & k = 0, 1, 2, 3, 4 \\ 0, & \text{para otros valores} \end{cases}$$

   a. Calcule $P(X = 3)$
   b. Calcule $P(1 \leq X \leq 2.5)$
   c. Calcule $P(X \leq 2.5)$

9. Sea X una variable aleatoria, cuya función de densidad se define como:

$$f(x) = \begin{cases} 0.2, & -1 \leq x \leq 0 \\ 0.2 + ax, & 0 < x \leq 1 \\ 0, & \text{para otros valores} \end{cases}$$

   a. Determine el valor de a.
   b. Encuentre la función de distribución $F_X(x)$
   c. Calcule $Pr(0 \leq X \leq 0.5)$
   d. Calcule $Pr(X > 0.5 \,|\, X > 0.1)$

Contenido

Introducción

Cuando se estudia las estructuras algebraicas se observan que ciertos sistemas matemáticos particulares comparten las mismas propiedades. La palabra “Grupo” en matemática es un término que dista mucho del concepto que se tiene de “Grupo” del lenguaje común.

Definición

Sea G un conjunto no vacío y $*$ una operación binaria definida en G. El par $(G, *)$ recibe el nombre de **Grupo** si se satisfacen las condiciones siguientes:

a. $\forall\, a, b \in G, \;\; a * b \in G.$ (Cierre de G respecto a *.)

b. $\forall\, a, b, c \in G, \;\; a * (b * c) = (a * b) * c.$ (Propiedad asociativa.)

c. $\exists\, e \in G \ \ni \ a * e = e * a = a, \ \forall\, a \in G.$ (Existencia elemento neutro o identidad.)

d. $\forall\, a \in G, \ \exists\, a^{-1} \in G \ \ni a * a^{-1} = a^{-1} * a = e.$ (Existencia de simétrico.)

Es importante hacer notar que cuando la operación del grupo es la suma (+), el simétrico, a^{-1} de un elemento a es $-a$.
Si $\forall\, a, b \in G$ se tiene que $a * b = b * a$, al grupo G se le llama **Grupo conmutativo o abeliano**.

Ejemplo 1

Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos abelianos con la operación suma (+) ordinaria. Sin embargo, ninguno es grupo con la operación de multiplicación ordinaria, puesto que 0 no tiene simétrico multiplicativo.

Ahora bien, si excluimos el 0 de los conjuntos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, se forman los conjuntos $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, respectivamente, los cuales son grupos abelianos multiplicativos.

Ejemplo 2

Sea $G = \{a, b, c, d, e\}$ un conjunto y $*$ una operación binaria definida por la tabla siguiente:

$*$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

Es claro que el conjunto G es un grupo con respecto a la operación $*$. El elemento neutro de la operación $*$ es a. El elemento simétrico de:

a es a

b es e

c es d

d es c

e es b

Ejemplo 3

Sea $G = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ un conjunto y $*$ la operación suma $(+)$ ordinaria de $\mathbb{Z}$. Este conjunto no es un grupo, porque aunque el 0 es el elemento neutro, cada elemento tiene su simétrico y es asociativa. Sin embargo, $+$ no es una operación binaria en G.

Ejemplo 4

Sea $G = \left\{ \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}, 1 \right\}$. Se puede comprobar que G es un grupo con respecto a la multiplicación en $\mathbb{C}$.

Ejemplo 5

Sea $G = \mathbb{Z}_n, \ n \in \mathbb{Z}$ y $+$ la operación suma ordinaria. El conjunto G es un grupo abeliano con respecto a $+$, como se puede comprobar en siguiente tabla para $n = 5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Ejemplo 6

Sea $G = \{(0,0),(0,1),(1,0),(1,1)\}$ y $*$ una operación definida en G como

$$(a,b) * (c,d) = (a \oplus c, b \oplus d),$$

donde $\oplus$ es la suma en $\mathbb{Z}_2$. Entonces el par $(G,*)$ es un grupo (grupo 4 de Klein). La siguiente tabla muestra la operación $*$:

$*$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Definición

Sea $(G, *)$ un grupo. Si G es un conjunto finito, a $(G, *)$ se le llama **Grupo finito**. Si $(G, *)$ es un grupo finito al número de elementos de G se le llama **Orden** de G y se representa por $|G|$.

Ejemplo 7

Si $n \in \mathbb{Z}^+$ se tiene que $|(\mathbb{Z}_n, +)| = n$.

Es común representar la operación del grupo en forma multiplicativa, por lo que a partir de este momento utilizaré esta forma. Es decir, en lugar de escribir $a * b$, se escribirá ab.

Algunas propiedades de grupos

Sea G un grupo. Entonces

a. el elemento neutro (identidad) (e) en G es único.

b. sea $a \in G$. El simétrico de a es único.

c. si $a, b, c \in G$ y $ab = ac$, entonces $b = c$.

d. si $a, b, c \in G$ y $ba = ca$, entonces $b = c$.

e. sean $a, b \in G$. G es abeliano, si y sólo si, $(ab)^2 = a^2 b^2$.

f. $\forall a \in G, \;\; (a^{-1})^{-1} = a$.

g. si $a, b \in G, \;\; (ab)^{-1} = b^{-1} a^{-1}$.

Sea $a \in G$ y $m \in \mathbb{Z}^+$. Entonces definimos

a. $a^m = a\, a\, a \cdots a$ (m veces).

b. $a^0 = e$ (elemento neutro).

c. $a^{-m} = (a^{-1})^m = a^{-1}\, a^{-1}\, a^{-1} \cdots a^{-1}$ (m veces)

Sean $m, n \in \mathbb{Z}$. Entonces

a. $a^m\, a^n = a^{m+n}$

b. $(a^m)^n = a^{mn}$

Sea $a \in G$. Se llama **Orden de** a al menor entero positivo n, si este existe, tal que $a^n = e$ (elemento neutro de G). Como ejemplo, podemos ver que el elemento

$$\frac{-1+\sqrt{3}i}{2}$$

del ejemplo 4 es de orden 3, puesto que

$$\left(\frac{-1+\sqrt{3}i}{2}\right)^3 = 1.$$

Recuerde que el 1 es el elemento neutro de este grupo.

Definición

Sea $(G, *)$ un grupo y sea $G' \subseteq G$ no vacío. Si $(G', *)$ es también un grupo, se le llama **Subgrupo** de $(G, *)$. Es claro que $G' = \{e\}$ y G son subgrupos de G y se les llama subgrupos **Triviales o impropios** de G. Observe que todo subgrupo de G contiene a e como elemento neutro.

Ejemplo

Considere el grupo $G = \{-1, 1, -i, i\}$ con respecto a la multiplicación. Un subgrupo propio de G es $G' = \{-1, 1\}$

Ejemplo

El grupo $(\mathbb{Z}_6, +)$ tiene como subgrupo el conjunto $G' = \{0, 2, 4\}$ con respecto a la misma operación de suma (+). Esto se puede observar en la siguiente tabla

$+$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Se puede comprobar que el conjunto $S = \{0, 3\}$ es también un subgrupo de $(\mathbb{Z}_6, +)$.

El grupo $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$. De la misma manera $(\mathbb{Q}, +)$ es un subgrupo de $(\mathbb{R}, +)$.

Ejemplo

Considere el grupo $(\mathbb{Z}_{10}, \oplus)$. Aquí $\oplus$ es la adición en $\mathbb{Z}_{10}$. Los subgrupos de $(\mathbb{Z}_{10}, \oplus)$ son

$$G' = \{0\}, \qquad G'' = \{0,1,2,3,4,5,6,7,8,9\}, \qquad G''' = \{0,5\}, \qquad G^{IV} =$$

Teorema

Sea G' un subconjunto no vacío de un grupo $(G, *)$. G' es un subgrupo de G, si y sólo si

a. G' es cerrado con respecto a $*$.

b. $\forall a \in G', \ \ a^{-1} \in G'$.

Teorema

Sea G' un subconjunto no vacío de un grupo $(G, *)$. G' es un subgrupo de G, si y sólo si, $\forall a, b \in G', \ \ a^{-1} * b \in G'$.

Contenido

Definición

Un grupo $(G, *)$ se le llama **Cíclico**, si existe un $a \in G$ tal que todo elemento $x \in G$ es de la forma $x = a^m, \;\; m \in \mathbb{Z}$. Al elemento a se le llama un **Generador** de G. Es lógico pensar que todo grupo cíclico es abeliano.

Ejemplo

El grupo $(\mathbb{Z}, +)$ es cíclico con generador $a = 1$, puesto que $\forall m \in \mathbb{Z}, \;\; a^m = ma = m.$

Contenido

Definición

Sean $(G, \circ)$ y $(G', *)$ dos grupos. Una función $f : G \to G'$ tal que $f(a \circ b) = f(a) * f(b), \ \ \forall\, a, b \in G$ se le llama **Homomorfismo de G en G'**. Se dice que G y G' son **Homomorfos.**

Si tanto $\circ$ como $*$ son las operaciones de adición (+), se tiene que

$$f(a + b) = f(a) + f(b).$$

Si $G = G'$, al homomorfismo se le llama **Endomorfismo**. Si el homomorfismo es inyectivo, se le llama **Monomorfismo** y si es sobreyectivo, se le llama **Epimorfismo**.

Ejemplo

Sean $(\mathbb{R}, +)$ y $(\mathbb{R}_0, \cdot)$ los grupos aditivo y multiplicativo ($\mathbb{R}_0$ representa los reales no nulos), respectivamente. La función $f : \mathbb{R} \to \mathbb{R}_0$ definida por $f(x) = e^x$ es un homomorfismo de $\mathbb{R}$ en $\mathbb{R}_0$, puesto que

$$\forall a, b \in \mathbb{R} : \quad f(a + b) = e^{a+b} = e^a \cdot e^b = f(a) \cdot f(b).$$

Ejemplo

Sean $(G = \{1\}, \cdot)$ y $(G' = \{0\}, +)$ grupos multiplicativo y aditivo, respectivamente. La función $f : G \to G'$ definida por $f(x) = 0$ es un homomorfismo de G en G'. De igual forma, la función $f : G' \to G$ definida por $f(x) = 1$ es un homomorfismo de G' en G. A estos se les llama **Homomorfismos triviales**.

Ejemplo

Sea $(G, *)$ un grupo. La función $I : G \to G$, definida por $I(x) = x$ es un homomorfismo y se le llama **Homomorfismo idéntico.**

Ejemplo

Sean $(G = \mathbb{Z}, +)$ y $(G' = \{-1, 1, -i, i\}, \cdot)$ grupos aditivo y multiplicativo, respectivamente. La función $f : G \to G'$ definida por $f(x) = i^x$ es un homomorfismo.

Ejemplo

Sea G un grupo abeliano cualquiera y sea $f : G \to G$, definida por $f(a) = a^2$. Es claro que f es un homomorfismo, puesto que

$$f(ab) = (ab)^2 = a^2\, b^2 = f(a)f(b).$$

Ejemplo

Sean $(G = \mathbb{Z}, +)$ y $(G' = \{-1, 1\}, \cdot)$ dos grupos. La función $f : G \to G'$, definida por $f(n) = (-1)^n$ es un homomorfismo, puesto

$$f(m+n) = (-1)^{m+n} = (-1)^m (-1)^n = f(m) f(n).$$

Definición

Sean $(G, \circ)$ y $(G', *)$ dos grupos. Sea $f : G \to G'$ un homomorfismo de G en G' y sea e' el elemento neutro de G'. Se llama **Núcleo** de f al conjunto

$$ker(f) = \{x \in G \,|\, f(x) = e'\}.$$

Sea $A \subseteq G$. Se llama **Imagen de** A mediante f al conjunto

$$f(A) = \{y \in G' \,|\, y = f(x), \;\; x \in A\}.$$

Al conjunto $f(G)$ se le llama **Imagen del homomorfismo.**

Sea $B \subseteq G'$. Al conjunto

$$f^{-1}(B) = \{x \in G \,|\, f(x) \in B\},$$

se le llama **Imagen inversa de** B mediante f.

Si todo $g' \in G'$ es imagen, se dice que G' es una **Imagen homomorfa** de G.

Teorema

Sean $(G, \circ)$ y $(G', *)$ dos grupos con sus identidades e y e', respectivamente. Si $f : G \to G'$ es un homomorfismo, entonces

a. $f(e) = e'$

b. $f(a^{-1}) = [f(a)]^{-1}, \ \forall\, a \in G$

c. $\forall A$ subgrupo de G, $f(A)$ es un subgrupo de G'

La demostración se deja como investigación para el lector.

Contenido

Definición

Sean $(G, \circ)$ y $(G', *)$ dos grupos. Se dice que $f : G \to G'$ es un **Isomorfismo**, si f es un homomorfismo biyectivo. En tal caso se dice que G y G' son grupos **Isomorfos**.

Ejemplo

Sean $(\mathbb{R}^+, \cdot)$ y $(\mathbb{R}, +)$ los grupos multiplicativo y aditivo. La función $f : \mathbb{R}^+ \to \mathbb{R}$, definida por $f(x) = \ln(x)$ es biyectiva (inyectiva y sobreyectiva). Sean $a, b \in \mathbb{R}^+$,
$f(ab) = \ln(ab) = \ln(a) + \ln(b) = f(a) + f(b)$. Por tanto, f es un isomorfismo.

Ejemplo

Sea $(G, *)$ un grupo cíclico de orden 3, donde $G = \{e, a, a^2\}$ y la operación viene definida por la siguiente tabla:

$*$	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

La función $f : G \to G$, definida por $f(e) = e, \quad f(a) = a^2, \quad f(a^2) = a$ es un isomorfismo de G en si mismo. Comprobemos que es un homomorfismo primeramente. $f(ee) = f(e)f(e) = e^2 = e$
$f(ea) = f(e)f(a) = ea^2 = a^2$
$f(ea^2) = f(e)f(a^2) = ea = a$

$f(aa^2) = f(a)f(a^2) = a^2a = e$

Puede observarse que también es inyectiva y sobreyectiva. Por tanto, es un isomorfismo de G en si mismo **(Automorfismo).**

Contenido

Definición

Un conjunto no vacío A es un **Anillo** respecto a las operaciones binarias de suma $(+)$ y multiplicación $(\cdot)$, si para todo $a, b, c \in A$, se satisfacen las siguientes propiedades:

a. $a + b = b + a$ Prop. conm. de $+$.

b. $a + (b + c) = (a + b) + c$ Prop. asoc. de $+$.

c. $\exists\, z \in A \ni a + z = z + a = a, \ \forall a \in A$ Exist. ident. $+$.

d. $\forall a \in A, \exists\, a' \in A \ni a + a' = a' + a = z$ Exist. inv. en $+$.

e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ Prop. asoc. de $\cdot$.

f. $a \cdot (b + c) = a \cdot b + a \cdot c$ Prop. dist. de $\cdot$ respecto a $+$.

g. $(b + c) \cdot a = b \cdot a + c \cdot a$ Prop. dist. de $\cdot$ respecto a $+$.

Se escribe $(A, +, \cdot)$. Observe que las operaciones $+$ y $\cdot$ pudieran no ser la suma y multiplicación ordinarias.

Ejemplo 1

Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con las operaciones ordinarias de suma y multiplicación son anillos. La identidad de la adición es el cero y el inverso aditivo de un elemento cualquiera a es $-a$.

Ejemplo 2

Sea $A = \{a, b\}$. Suponga que las operaciones $+$ y $\cdot$ se definen por las siguientes tablas:

$+$	a	b
a	a	b
b	b	a

y

$\cdot$	a	b
a	a	a
b	a	b

Se puede comprobar que efectivamente es un anillo.

Ejemplo 3

Sea $A = \{a, b, c, d\}$. Suponag que las operaciones $+$ y $\cdot$ se definen mediante las tablas siguientes:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

y

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

Se puede comprobar que efectivamente es un anillo.

Ejemplo 4

Sea $A = \mathbb{Z}^{2\times 2}$ el conjunto de todas las matrices de orden 2, cuyos elementos pertenecen a $\mathbb{Z}$. En este conjunto, la igualdad ocurre si y sólo si sus elementos respectivos son iguales. Suponga que las operaciones de $+$ y $\cdot$ vienen dadas por:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Con estas operaciones, el conjunto A es un anillo. El elemento identidad aditivo es

$$z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

El inverso de

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ es } \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

Con frecuencia, en lugar de escribir $a \cdot b$ se escribe ab.

Definición

Sea $(A, +, \cdot)$ un anillo con elemento cero z. Entonces se dice que un elemento $a \in A, \quad a \neq z$ es un **Divisor de cero**, si existe un elemento $b \neq z$ en A, tal que $a \ \cdot \ b = z$ o $b \ \cdot \ a = z$.

Ejemplo

Los anillos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ Y $\mathbb{C}$ no tienen divisores de cero, puesto que siempre que $ab = 0$, ocurre que $a = 0$ o $b = 0$.

Definición

Sea $(A, +, \cdot)$ un anillo.

a. $\forall\, a, b \in A$, si $ab = ba$, se dice que A es un anillo **conmutativo.**

b. A no tiene divisores propios de cero, si $\forall\, a, b \in A, \;\; ab = z \Rightarrow a = z$ o $b = z$.

c. Si $\exists u \in A \;\ni\; au = ua = a, \;\; \forall a \in A$, a u se le llama **Unitario o identidad multiplicativa** de A. A A se le llama **Anillo con unitario.**

Los anillos del primer ejemplo de esta sección son conmutativos con unitario (1). No tienen divisores propios de cero. El ejemplo 4 no es conmutativo. Tiene como unitario la matriz

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

y contiene divisores propios de cero.

Ejemplo

Sea $U = \{a, b\}$ y $A = P(U)$. Sean $S, T \subseteq P(U)$. Suponga que se definen las operaciones $+$ y $\cdot$ como

$$S + T = S \Delta T = \{x \,|\, x \in (S \cup T) \text{ y } x \notin (S \cap T)\}$$

$$S \cdot T = S \cap T \ \ \text{(intersección)}$$

Las tablas correspondientes a las operaciones se definen como:

$+$	$\emptyset$	$\{a\}$	$\{b\}$	U
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	U
$\{a\}$	$\{a\}$	$\emptyset$	U	$\{b\}$
$\{b\}$	$\{b\}$	U	$\emptyset$	$\{a\}$
U	U	$\{b\}$	$\{a\}$	$\emptyset$

y

$\cdot$	$\emptyset$	$\{a\}$	$\{b\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
U	$\emptyset$	$\{a\}$	$\{b\}$	U

Se comprueba que A es un anillo conmutativo finito con unitario. Como ejemplos de divisores de cero se tiene los elementos $\{a\}$ y $\{b\}$. Aquí el elemento $\emptyset$ es la identidad aditiva y cada elemento es su propio inverso.

Definición

Sea A un anillo con unitario u. Sean $a, b \in A$. Si $a\,b = b\,a = u$, se dice que b es el **Inverso multiplicativo** de a. A a se le llama **Unidad** de A.

Definición

Sea A un anillo con unitario. Entonces se dice que:

a. A es un **Dominio entero**, si A no tiene divisores propios de cero.

b. A es un **Campo**, si todo elemento de A diferente de cero es una unidad.

Atendiendo a esta definición podemos decir que $(\mathbb{Z}, +, \cdot)$ es un dominio entero, pero no un campo. Los conjuntos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ con las operaciones de suma y multiplicación ordinarias son dominios enteros y campos.

Sea $(A, +, \cdot)$ un anillo. Entonces

a. A es un grupo aditivo abeliano.

b. Existe un elemento neutro aditivo único z.

c. Cada elemento tiene un simétrico aditivo único.

d. Para la suma se cumple la ley de cancelación.

e. $-(-a) = a, \;\; -(a+b) = (-a) + (-b), \;\; \forall a, b \in A$.

f. $a \cdot z = z \cdot a = z$

g. $a \cdot (-b) = -(ab) = (-a) \cdot b$.

Definición

Sea $(A, +, \cdot)$ un anillo. Un **Subanillo** de A es cualquier subconjunto no vacío S de A que sea a su vez anillo respecto a las operaciones binarias de A. Si S es un subanillo del anillo A, entonces S es un subgrupo del grupo aditivo A.

Ejemplo

El conjunto $\mathbb{Z}$ es un subanillo de los anillos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. De la misma forma $\mathbb{Q}$ es un subanillo de $\mathbb{R}$ y $\mathbb{C}$. $\mathbb{R}$ es un subanillo de $\mathbb{C}$.

Los subanillos $\{z\}$ y A mismo de un anillo A se dicen **Impropios o triviales**. Si hay otros subanillos se les llama **Propios**

Sea $(A, +, \cdot)$ un anillo. Sea T un subconjunto propio de A. T es un subanillo de A, si y sólo si, se satisfacen las condiciones siguientes:

a. $\forall a, b \in T : \quad (a + b) \in T,$ y $a \cdot b \in T$ (Cerradura)

b. $\forall a \in T : \quad -a \in T$

Definición

Sea $(A, +, \cdot)$ un anillo con elemento cero z. Suponga que para todo $a \in A$, existe un entero positivo k tal que $ka = a + a + \cdots + a = z$. Al menor entero positivo k para el cual se cumple la ecuación anterior se le llama **Característica** de A. Si el entero k no existe, se dice que A tiene característica cero.

Ejemplo

Los anillos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ tienen característica cero, puesto que $ka = k \cdot a$.

Contenido

Definición

Sean $(A, +, \cdot)$ y $(B, \oplus, \odot)$ dos anillos. Un **Homomorfismo de anillos** es una función $f : A \to B$ tal que para toda $a, b \in A$ se satisface las siguientes condiciones:

a. $f(a + b) = f(a) \oplus f(b)$.
b. $f(a \cdot b) = f(a) \odot f(b)$.

Es decir que esta función preserva las operaciones de anillos.

Definición

Sean $(A, +, \cdot)$ y $(B, \oplus, \odot)$ dos anillos. Suponga que $f : A \to B$ es un homomorfismos de anillos. Si f es inyectiva y sobreyectiva, se le llama **Isomorfismo de anillos** y se dice que A y B son anillos **Isomorfos**.

Ejemplo

Sea $A = \{a, b, c, d, e\}$ y definamos las operaciones $+$ y $\cdot$ mediante las tablas:

$+$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

y

$\cdot$	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

Este conjunto junto a estas operaciones, es un anillo conmutativo finito con unitario y sin divisores propios de cero. El elemento a es el cero de A y b es el unitario. Todo elemento distinto de cero tiene un inverso multiplicativo y $xy = yx = b$. c y d son inversos multiplicativos recíprocos y b es su propio inverso, al igual que e.

Considérese el anillo A anterior y el anillo $\mathbb{Z}_5$. Entonces la función $f : A \to \mathbb{Z}_5$, definida por

$$f(a) = [0], \quad f(b) = [1], \quad f(c) = [2], \quad f(d) = [3], \quad f(e) = [4]$$

es un isomorfismo de anillos.

Observemos que

$$f(c+d) = f(a) = [0] = [2] + [3] = f(c) + f(d)$$

y

$$f(be) = f(e) = [4] = [1][4] = f(b)f(e).$$

De la misma manera se puede seguir comprobando las demás igualdades (son 25).

Ejemplo

Sea $A\{a, b, c, d\}$ y definamos las operaciones $+$ y $\cdot$ mediante las tablas siguientes:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

y

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

Sea $B = \{p, q, r, s\}$ y las operaciones $\oplus$ y $\odot$ definidas mediante las siguientes tablas:

$\oplus$	p	q	r	s
p	r	s	p	q
q	s	r	q	p
r	p	q	r	s
s	q	p	s	r

y

$\odot$	p	q	r	s
p	s	p	r	q
q	p	q	r	s
r	r	r	r	r
s	q	s	r	p

La función $f : A \to B$, definida por

$$f(a) = r, \quad f(b) = q, \quad f(c) = s, \quad f(d) = p$$

es un isomorfismo. Observe que

$$f(b + c) = f(d) = p = f(b) \oplus f(c) = q \oplus s$$

y

$$f(c \cdot d) = f(b) = q = f(c) \odot f(d) = s \odot p.$$

Se pueden comprobar las demás igualdades.

1. Determine si el conjunto $\mathbb{Z}_5$ forma un grupo respecto a las operaciones de adición y multiplicación. Si es así, encuentre el neutro y simétrico de cada elemento.
2. Sean $a, b, c \in G$. Demuestre que si $a * b = a * c$, entonces $b = c$.
3. Sean $a, b, c \in G$. Demuestre que si $b * a = c * a$, entonces $b = c$.
4. Sean $a, b \in G$. Demuestre que las ecuaciones $a * x = b$ y $y * a = b$ tienen soluciones únicas.
5. Sea $A = \mathbb{Z}$ y considérese la operación $+$ definida como sigue:

$$a + b = a + b - 8.$$

   Determine si $(A, +)$ es un grupo conmutativo.

6. Sea $A = \mathbb{Z}$ y considérese la operación $\cdot$ definida como sigue:

$$a \cdot b = a + b - a \cdot b.$$

   Determine si $(A, \cdot)$ es un subgrupo conmutativo.

7. ¿Cuáles de los siguientes conjunto forman grupo, respecto a la operación indicada.
   a. $T = \{x \,|\, x \in \mathbb{Z},\ x < 0\}$ adición.
   b. $T = \{7x \,|\, x \in \mathbb{Z},\}$ adición.
   c. $T = \{-2, -1, 0, 1, 2\}$ multiplicación.
   d. $T = \{-1, 1, -i, i\}$ multiplicación.
   e. $\mathbb{Z}_m$ adición.
   f. $\{-1, 1\}$ adición.
   g. $\{-1, 1\}$ multiplicación.

8. El conjunto $\{[1], [5], [8], [12]\}$ es un subconjunto de $\mathbb{Z}_{13}$. Determine si es un grupo con respecto a la multiplicación.
9. Sean $a, b \in G$. Pruebe que:
   a. $(a^{-1})^{-1} = a$
   b. $(a\,b)^{-1} = b^{-1}\,a^{-1}$
10. Encuentre todos los subgrupos de $(\mathbb{Z}_{12}, +)$ y $(\mathbb{Z}_{11}^{*}, \cdot)$ (no considera el cero).
11. Compruebe que $(\mathbb{Z}_{p}^{*}, \cdot)$ es cíclico para los primos 5, 7,y 11.
12. Encuentre los generadores de los grupos cíclicos $(\mathbb{Z}_{12}, +)$ y $(\mathbb{Z}_{16}, +)$.
13. Si G es un grupo de orden n y $a \in G$, demuestre que $a^{n} = e$.

14. Sea $\mathbb{Z}^{2\times 2}$ el anillo de las cuadradas de orden 2, cuyos elementos son enteros. Si

$$A = \begin{pmatrix} 4 & 7 \\ 1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix},$$

encuentre $A^{-1}, \quad B^{-1}, \quad (A\,B)^{-1}, \quad (B\,A)^{-1}, \quad B^{-1}\,A^{-1}$

15. Pruebe que

$$T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \,\middle|\, a \in \mathbb{Z} \right\}$$

es un subanillo de $\mathbb{Z}^{2\times 2}$.

16. Sea A el conjunto de los enteros pares. Considere las operaciones de suma ordinaria $(+)$ y $\cdot$ definida como

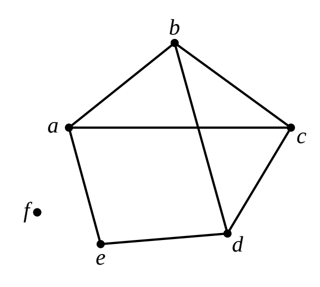
$$a \cdot b = \frac{a\,b}{2}.$$

Demuestre que $(A, +, \cdot)$ tiene estructura de anillo.

La teoría de grafos empieza a estudiarse formalmente en el siglo XVIII, específicamnete a partir del año 1736, a raíz de un artículo escrito por Leonhard Euler (1707 - 1783) sobre lo que hoy se conoce el problema de los siete (7) puentes de Königsberg (hoy Kaliningrado). Parece que la inquietud que subyace en la cabeza de Euler al salir de su casa en la margen derecha del río Pregel, el cual tiene siete puentes que comunican ambas mŕgenes del río con dos islas. La más pequeña se comunica con ambos lados del río a través de dos (2) puentes; la más grande se comunica con ambas márgenes por medio de cuatro (4) puentes (dos a ambos lados) y ellas que se comunican entre si a través de un puente. Euler caminaba con frecuencia a ambos lados del río, pasando por estos puentes y la pregunta que le surge es: ¿ cómo regresar a su casa sin pasar dos veces por un mismo puente?.

Cuando deseamos hacer un recorrido por varios pueblos del país lo primero que nos viene a la cabeza es tomar un mapa para observar las rutas o carreteras que los comunican. Este es un problema propio de la teoría de grafos donde sobresalen dos conjuntos diferentes: el conjunto de los pueblos a visitar y el conjunto de carreteras. Con estos conjuntos podemos establecer una relación: si a y b son pueblos, entonces a está relacionado con b, si hay una carretera que los comunica. Si además la carretera es de doble vía, entonces también se tiene que b está relacionado con a. Si todas las carreteras son de doble vías, se tiene que la relación es simétrica.

La figura siguiente es una representación gráfica de esto último.

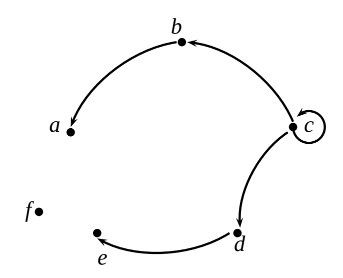


Definición

Un **Grafo dirigido o digrafo** es un par $G = (V, A)$, donde V es un conjunto finito no vacío, llamado conjunto de **Vértices o nodos** y $A \subseteq V \times V$, llamado conjunto de **Aristas.**

Ejemplo

Sean $V = \{a, b, c, d, e, f\}$ y $A = \{(c, b), (b, a), (c, c), (c, d), (d, e)\}$. Entonces $G = (V, A)$ es un grafo dirigido, representado por la figura siguiente:



Definición

Se dice que un vértice v y una arista a de un grafo G son **Incidentes** si v es un extremo de a. EL **Grado o valencia** de un vértice v es la cantidad de aristas incidentes en v, es decir, el número de aristas que tienen a v como extremo. El grado del vértice v lo representamos por $gr(v)$. Un vértice v se dice **Aislado** si $gr(v) = 0$. Un vértice v se dice **Pendiente** si $gr(v) = 1$. Cuando todos los vértices de un grafo G tienen el mismo grado, digamos m, decimos que el grafo es m-**regular**.

Por ejemplo, en el grafo del ejemplo anterior, la arista (c, d) es incidente con los vertices c y d, el grado del vértice a, $gr(a) = 1$ (pendiente) y el $gr(f) = 0$ (aislado).

Teorema

En todo grafo G el número de vértices de grado impar es par.

Demostración

Sea $G = (V, A)$ un grafo. Sean $V_i = \{v \in V \mid gr(v)$ es impar$\}$ y $V_p = \{v \in V \mid gr(v)$ es par$\}$. Se sabe que toda arista es incidente en dos vértices, por tanto

$$2|A| = \sum_{v \in V} gr(v) = \sum_{v \in V_i} gr(v) + \sum_{v \in V_p} gr(v).$$

De donde

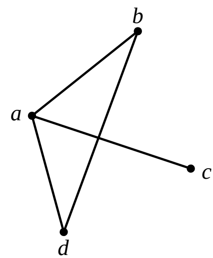
$$\sum_{v \in V_i} gr(v) = 2|A| - \sum_{v \in V_p} gr(v).$$

Esto nos dice que una suma de números impares produce un número par, ya que es la diferencia de dos pares, pero este caso sólo puede ocurrir si la cantidad de sumandos es par. Es decir, que $|V_i|$ es par. Esto completa la demostración.

Definición

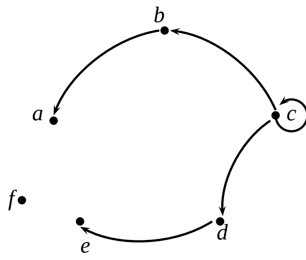
Sea $G = (V, A)$ un grafo. Se dice que los vértices v_1 y v_2 son **Adyacentes** si son extremos de la misma arista. Dos aristas son **Adyacentes** si tienen un vértice en común. Un **Lazo** es una arista donde ambos extremos coinciden. Los lazos se cuentan doble para los fines de calcular el grado de un vértice. Dos aristas son **Paralelas o mútiples** si coinciden en ambos extremos. Un grafo es **Simple o sencillo** si no tiene lazos ni aristas paralelas.

Por ejemplo, observe el grafo siguiente:



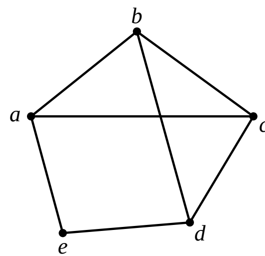
Los vértices b y d son adyacentes. Se dice que b es adyacente a d y que d es adyacente desde b.

En el grafo



La arista (c, c) es un lazo.

Si la dirección de una arista no tiene importancia, se dice que el grafo es **No dirigido**. Por ejemplo, el siguiente grafo es no dirigido.



Debe entenderse en el grafo que las aristas se dan en ambas direcciones, por ejemplo (a, b) y (b, a) son elementos del conjunto A de aristas. En los grafos no dirigidos, las aristas suelen escribirse en notación de conjuntos, por ejemplo, escribir la arista $\{c, d\}$ significa $\{(c, d), (d, c)\}$. Un lazo en el vértice c de un grafo no dirigido se escribe $\{c, c\}$.

Definición

Sea $G = (V, A)$ un grafo. La **Matriz de adyacencia** de G es la matriz $M_A(G)$ de orden $m \times m$, donde $m = |V|$, definida por

$$M_A(G) = \begin{cases} 0, & (v_i, v_j) \notin A \\ 1, & (v_i, v_j) \in A \end{cases}.$$

La **Matriz de incidencia** de G es la matriz $M_I(G)$, de orden $m \times n$, donde $m = |V|$ y $n = |A|$ y definida por

$$M_I(G) = \begin{cases} 0, & \text{si } \ v_i, a_j \ \text{ no son incidentes} \\ 1, & \text{si } \ v_i, a_j \ \text{ son incidentes} \end{cases}.$$

Ejemplo

Sea $G = (V, A)$ un grafo. Sean $V = \{a, b, c, d, e, f\}$ y $A = \{\{a, a\}, \{a, b\}, \{a, e\}, \{b, c\}, \{b, e\}, \{c, d\}, \{d, e\}, \{d, f\}\}$. Entonces las matrices de adyacencia e incidencia son respectivamente

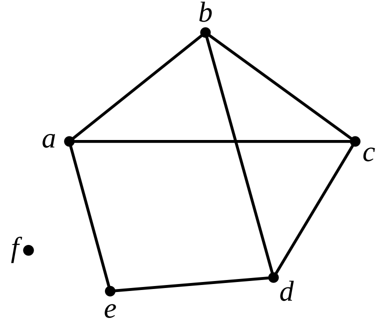
$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Definición

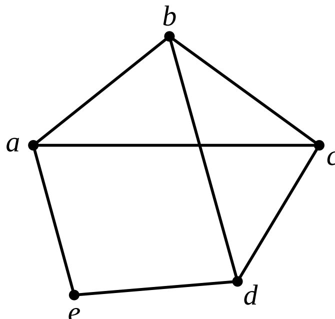
Sea $G = (V, A)$ un grafo no dirigido y sean $v, w \in V$. Un **Camino o cadena** de v a w en G es una sucesión finita no vacía de aristas distintas $\{v, x_1\}, \{x_1, x_2\}, \{x_2, x_3\}, \ldots, \{x_{i-1}, x_i\}, \ldots, \{x_{n-1}, x_n\}, \{x_n, w\}$. Se escribe $v - w$. Si $v = w$, al camino se le llama **Ciclo**. La cantidad de aristas de un camino se le llama **Longitud** del camino. Por ejemplo, en el grafo de la primera gráfica de esta sección, $\{a, b\}$, $\{b, d\}, \{d, c\}$ es un camino de a a c. Un camino **Simple** es aquel en el cual se cruza sólo una vez por cada vértice. Es decir, si dos vértices cualesquiera son unidos a lo más por una sola arista. Cuando el grafo es dirigido, se habla de camino dirigido. Es importante hacer notar que estos conceptos son también válidos para los ciclos.

Definición

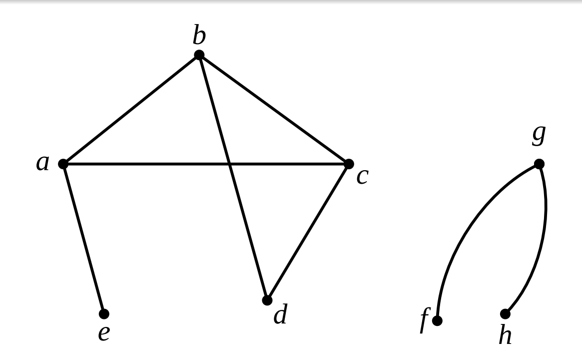
Sea $G = (V, A)$ un grafo no dirigido y sean $v, w \in V, v \neq w$. Decimos que G es **Conexo**, si existe un camino entre v y w. Si el grafo no es conexo, decimos que es **No conexo**. Por ejemplo, el grafo



es no conexo. El grafo de la figura siguiente es conexo.



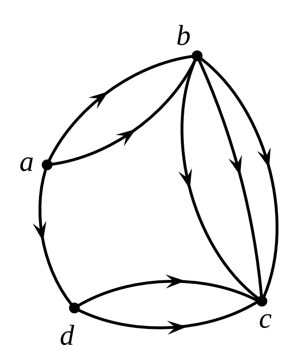
Un grafo es conexo si consta de una sola parte. El grafo de la siguiente figura es otro ejemplo de grafo no conexo porque está formado por más de una parte.



Definición

Decimos que un grafo $G = (V, A)$ es un **Multigrafo**, si hay $v, w \in V, \;\; v \neq w$, unidos por dos o más aristas de la forma (v, w) o de la forma $\{v, w\}$, dependiendo de si el grafo es dirigido o no dirigido,

respectivamente. Es decir, un multigrafo es un grafo donde hay pares de vértices unidos por más de una arista (tienen aristas múltiples). La figura siguiente es un ejemplo de multigrafo.



El número de aristas de v a w se le llama **Multiplicidad** de la arista (v, w). Así la arista (a, b) del grafo anterior es de multiplicidad 2 y la arista (b, c) es de multiplicidad 3.

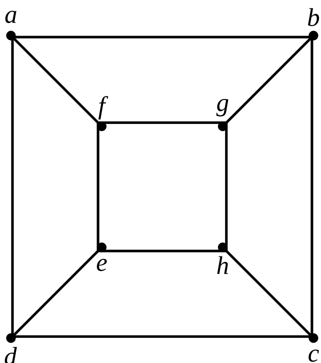
Sea $n \in \mathbb{Z}^+$. Un n-**grafo** es un grafo donde ninguna arista tiene multiplicidad mayor que n.

Para fines de notación, si V y A son los conjuntos de vértices y aristas respectivamente, de un grafo G, usaremos también la simbología $V(G)$ y $A(G)$ para indicar conjunto de vértices de G y conjunto de aristas de G, respectivamente.

1. Escriba un ejemplo de un grafo conexo G, en el que eliminando cualquier arista de G se obtenga un grafo no conexo.
2. Suponga un grafo que satisface la condición del ejercicio 1.
   a. ¿G tiene que ser un grafo sin lazos?.
   b. ¿Podría ser G un multigrafo?.
   c. Si G tiene n vértices, ¿se puede determinar cuántas aristas tiene?.
3. Si $G = (V, A)$ es un grafo no dirigido con $|V| = n$ y $|A| = m$ y sin lazos, demuestre que $2m \leq n^2 - n$.
4. Sea $G = (V, A)$ un grafo no dirigido. Defina una relación R en V donde aRb, si $a = b$ o existe un camino en G de a en b. Demuestre que R es una relación de equivalencia.

5. Si la suma de los grados de un grafo es 20, ¿cuántas aristas tiene el grafo?.
6. Suponga que los pueblos a, b, c, d, e, f, g están unidos por un conjunto de carreteras de la siguiente manera: la carretera C_1 va de a a c pasando por b; la carretera C_2 va de c a d continuando hacia f; la carretera C_3 va de d a a pasando por e; la carretera C_4 va de f a b pasando por g; y la carretera C_5 va de g a d.
   a. Dibuje un grafo que represente el sistema planteado.
   b. Exprese los caminos simples de g a a.
   c. ¿Cuál es el menor número de segmentos que habría que cerrar para interrumpir el paso de b a d?.
   d. ¿Es posible salir del pueblo c y regresar a él pasando una sola vez por los otros pueblos?.
   e. ¿Es posible salir del pueblo c sin necesidad de regresar al él?.

7. ¿Cuántos caminos simples diferentes existen entre los vértices f y c del siguiente grafo?.

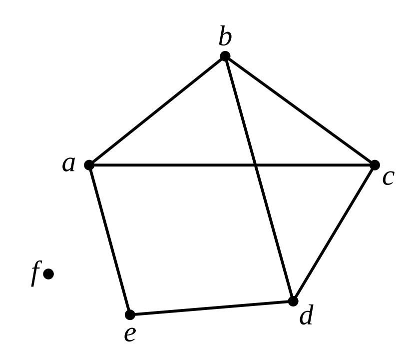


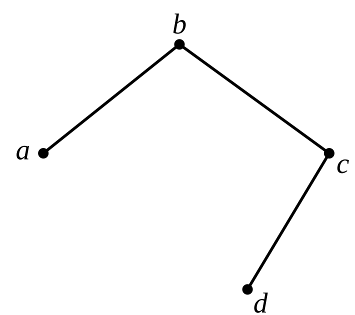
Contenido

Definición

Sea $G = (V, A)$ un grafo. Se llama **Subgrafo de** G al par $G' = (V', A')$, donde $V' \neq \emptyset$, $V' \subseteq V$ Y $A' \subseteq A$ y cada arista de A' es incidente con vértices de V'.

Ejemplo



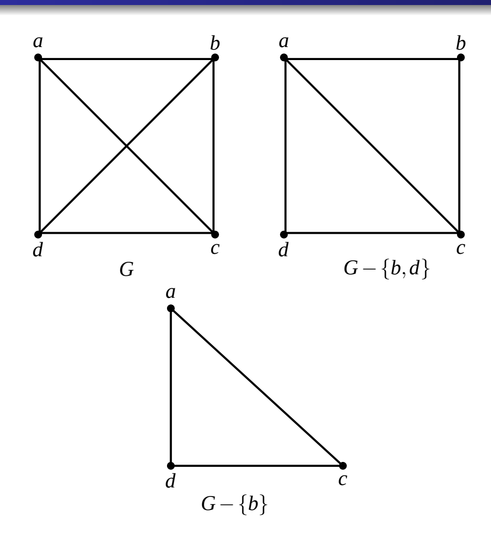


Observe que el segundo grafo es un subgrafo del primero.

Ejemplo

En este ejemplo tenemos un grafo G con dos subgrafos, como lo muestra la figura siguiente:

Subgrafos



Definición

Sean H y G dos grafos. Decimos que H es un **Subgrafo abarcador** de G, si

a. H es un subgrafo de G.

b. $V(H) = V(G)$.

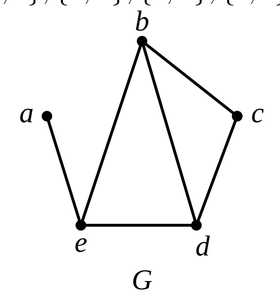
Definición

Sean H y G dos grafos y sea $V_1 \subseteq V(G)$. Decimos que H es un **Subgrafo inducido** de G, si

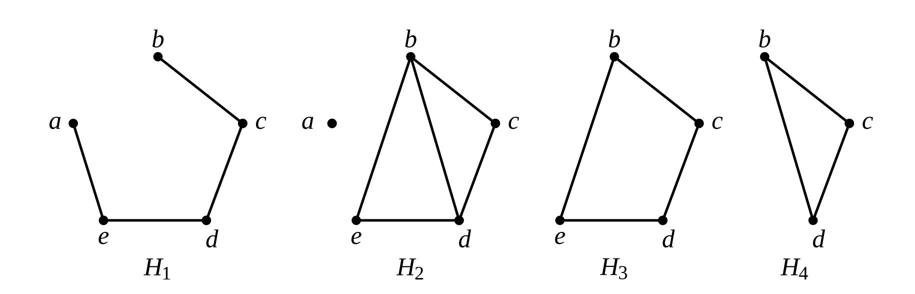
a. $V_1 = V(H)$.

b. si $v_1, v_2 \in V_1$ y $\{v_1, v_2\} \in A(G)$, entonces $\{v_1, v_2\} \in A(H)$

Por ejemplo, consideremos el grafo G de la siguiente figura. En este grafo, $V(G) = \{a, b, c, d, e\}$ y
$A(G) = \{\{b, c\}, \{c, d\}, \{d, e\}, \{e, a\}, \{b, d\}, \{b, e\}\}$.

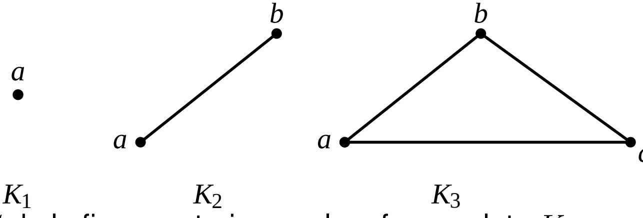


Los grafos H_1, H_2, H_3 y H_4 de la siguiente figura son subgrafos de G. H_1 y H_2 son subgrafos abarcadores de G. H_3 y H_4 son subgrafos inducidos de G.



Definición

Sea V un conjunto de n vértices. Se llama grafo **Completo** en V, al grafo no dirigido y sin lazos en el que para cualesquiera $v, w \in V, \; v \neq w$, existe una arista $\{v, w\}$. Se representa por K_n. Por ejemplo, los grafos K_1, K_2, K_3 son respectivamente



El grafo G de la figura anterior es el grafo completo K_4.

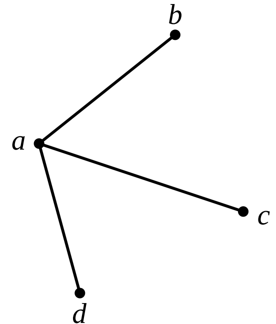
Contenido

Definición

Sea $G = (V, A)$ un grafo no dirigido sin lazos, donde V tiene n vértices. Se llama **Complemento** de G, al subgrafo de K_n formado por los n vértices de G y las aristas que no están en G. Se representa por G^c. Si $G = K_n$, entonces a G^c se le llama grafo **Nulo**, puesto que tiene n vértices y no tiene aristas.

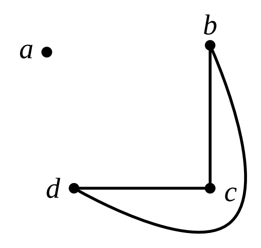
Ejemplo

Sea $V = \{a, b, c, d\}$ y $K_4 = (V, A_1)$ tal que $A_1 = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\}$ (hace las veces de un conjunto universal). Consideremos el grafo G definido por la figura:



Es decir, $G = (V, A_2)$, donde $A_2 = \{\{a, b\}, \{a, c\}, \{a, d\}\}$. Su complemento es el grafo representado por la siguiente figura:

Complemento



Es decir, el complemento de G es el grafo $G^c = (V, A_3)$, donde $A_3 = \{\{b, c\}, \{b, d\}, \{c, d\}\}$.

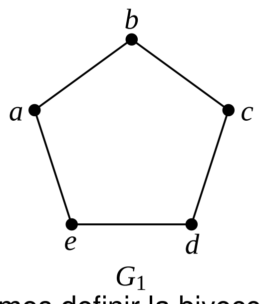
Contenido

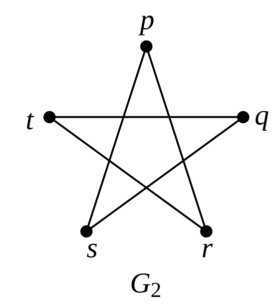
Definición

Sean $G_1 = (V_1, A_1)$ y $G_2 = (V_2, A_2)$ dos grafos no dirigidos. Un **Isomorfismo de grafos** es una función biyectiva $f : V_1 \to V_2$, tal que para todo $v, w \in V_1 : \{v, w\} \in A_1$, si y sólo si, $\{f(v), f(w)\} \in A_2$. En tal caso, se dice que G_1 y G_2 son **Grafos isomorfos**. En grafos isomorfos se conservan las adyacencias.

Ejemplo

Considere los grafos siguientes:





Ahora podemos definir la biyección :

$$f(a) = t, \quad f(b) = p, \quad f(c) = q, \quad f(d) = r, \quad f(e) = s.$$

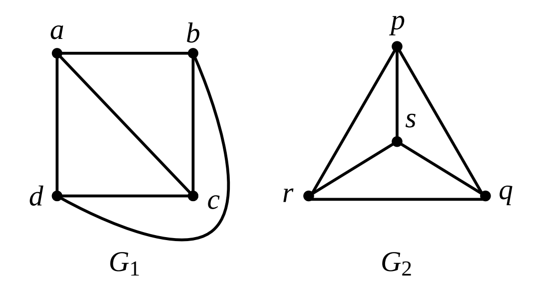
Esto nos dice que G_1 y G_2 son isomorfos.

Dos grafos $G_1 = (V_1, A_1)$ y $G_2 = (V_2, A_2)$ son isomorfos, si y sólo si, existe una permutación de vértices y aristas para la cual sus matrices de incidencias son iguales. Es fácilmente verificable que las matrices de incidencia de los grafos anteriores son iguales. Veamos

$$M_I(G_1) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad M_I(G_2) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ejemplo

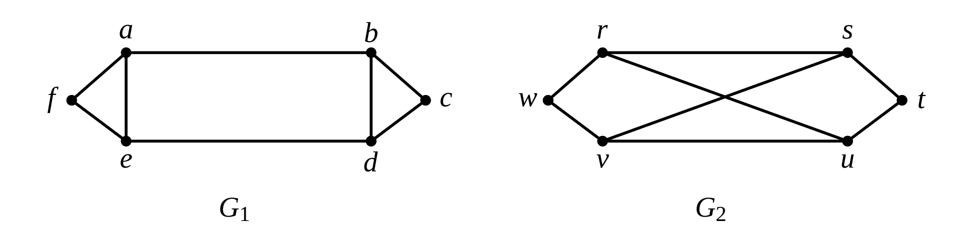
Consideremos los grafos de la figura siguiente:



Podemos definir la biyección $f(a) = p, \;\; f(b) = q, \;\; f(c) = s, \;\; f(d) = r$. Por tanto, los grafos G_1 y G_2 son isomorfos.

Ejemplo

Los grafos de la siguiente figura no son isomorfos:

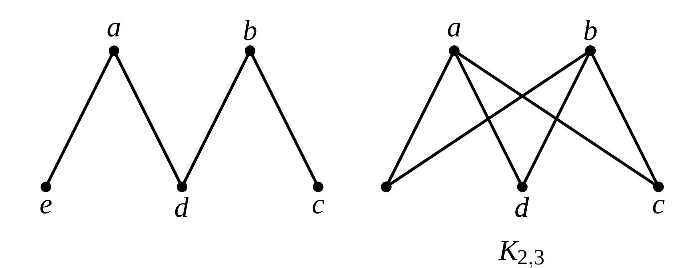


Definición

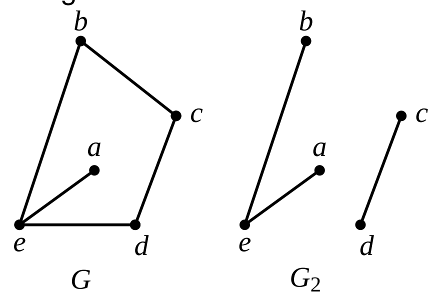
Un grafo $G = (V, A)$ se llama **Bipartito**, si existe una partición $\{V_1, V_2\}$ de V y cada arista $\{a, b\}$ de G tiene un vértice en V_1 y el otro en V_2. Cuando todo vértice de V_1 está unido a todo vértice de V_2, a G se le llama **Bipartito completo** y se representa por $K_{m,n}$, si $|V_1| = m$ y $|V_2| = n$.

Ejemplo

Sea $G = (V, A)$, donde $V = \{a, b, c, d, e\}$. Tomemos la partición, cuyos elementos son los conjuntos $V_1 = \{a, b\}$ y $V_2 = \{c, d, e\}$. La siguiente gráfica muestra un grafo bipartito y otro bipartito completo ($K_{2,3}$).


a
b
e
d
c
a
b
d
c
$K_{2,3}$

1. Considere los grafos siguientes:



   a. Escriba la matriz de adyacencia correspondiente a los grafos G_1 y G_2.

b. Suponga que A y B son las matrices de adyacencia que unen los nodos etiquetados con b, e y a, definidas por

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

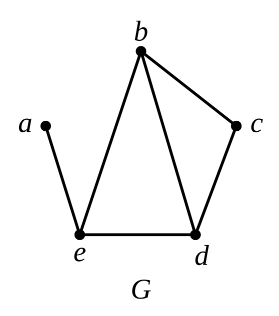
Encuentre los grafos asociados a dicha matrices de adyacencia.

c. Calcule $BA - AB$.

2. Sea $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$ y $A = \{(x, y) \Big| x \mid y,\ x < y\}$. Escriba el digrafo y la matriz de adyacencia asociada.

3. Sea $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$ y $A = \{\{x, y\} \Big| x$ y $y,$ tienen factor común en $V\}$. Escriba el grafo y la matriz de adyacencia asociada.
4. Sea $V = \{1, 2, 3, 4, 5, 6\}$ y $A = \{\{1, 2\}, \{1, 5\}, \{2, 3\}, \{2, 5\}, \{3, 4\}, \{4, 5\}, \{4, 6\}\}$. Encuentre
   a. Encuentre el grado de los nodos 1,2,3,y 4.
   b. Encuentre los vértices adyacentes.
   c. ¿Cuántos vecinos tiene cada vértice?.

5. Considere el grafo de la figura siguiente. Encuentre todos los caminos de b a a y determine la longitud de cada uno.

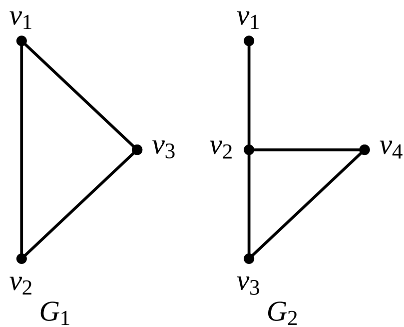


Ciclos y caminos de Euler

Decimos que un grafo o multigrafo no dirigido, $G = (V, A)$, tiene un **Ciclo de Euler**, si existe un ciclo simple en G que pasa por todo vértice $v \in V$ y por toda arista $a \in A$ solamente una vez. Un **Camino de Euler** es un camino en G que va de u a w y que pasa por todo vértice $v \in V$ y por toda arista $a \in A$ solamente una vez.

Ejemplos

Consideremos los grafos de la figura siguiente:



El grafo G_1 tiene un ciclo y un camino de Euler.

Ciclos y caminos de Hamilton

Decimos que un grafo o multigrafo no dirigido, $G = (V, A)$, tiene un **Ciclo de Hamilton**, si existe un ciclo simple en G que contenga todo vértice $v \in V$. Si existe un camino simple en G que contiene todos los vértices $v \in V$, a éste se le llama **Camino de Hamilton.**

Contenido

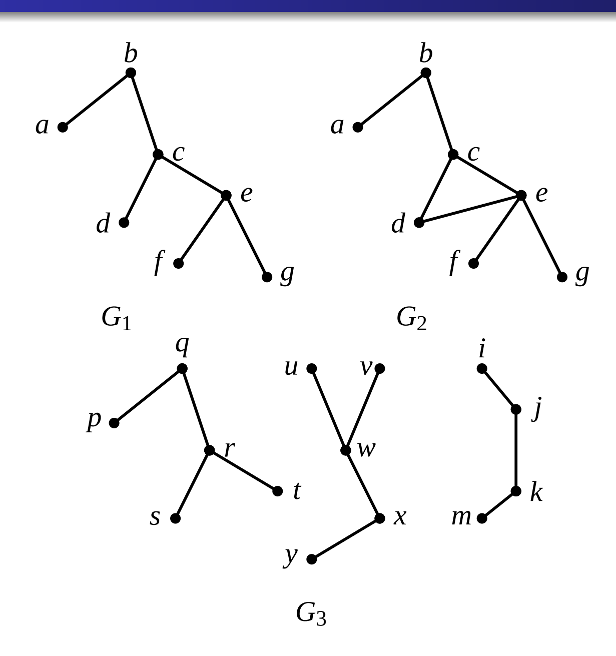
Definición

Un grafo $G = (V, A)$ no dirigido es un **Árbol** si es conexo y acíclico (no tiene ciclos).

Un **Bosque** es un grafo acíclico cuyas componentes son árboles.

Ejemplo

En la figura siguiente, G_1 es un árbol, G_2 no es un árbol porque tiene un ciclo y G_3 no es un árbol porque no es conexo. Sin embargo, G_3 es un bosque, donde cada parte es un árbol.


b
a
c
e
d
f
g
G_1
b
a
c
e
d
f
g
G_2
q
p
r
t
s
u
v
w
x
y
i
j
k
m
G_3

Al árbol G_1 que es un subgrafo de G_2 que contiene todos los vértices de G_2 se le llama **Árbol abarcador** de G_2.

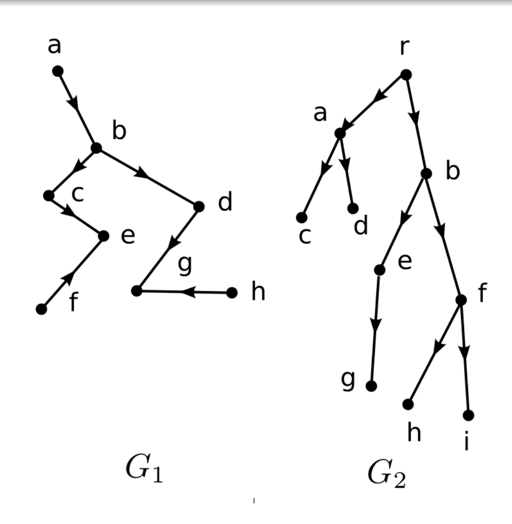
Definición

Un **Árbol dirigido** es un grafo dirigido G que se convierte en árbol al ignorar las direcciones de sus aristas. Un **Árbol con raíz** es un árbol dirigido G que tiene exactamente un vértice r, cuyo grado de entrada, $gr^+(r) = 0$, y teniendo los demás vértices v grado de entrada, $gr^+(v) = 1$. Al vértice r se le llama **Vértice raíz.**

Ejemplo

En la siguiente figura, el grafo G_1 es un árbol que no tiene raíz y G_2 es un árbol con raíz r.

Árboles con raiz



Contenido

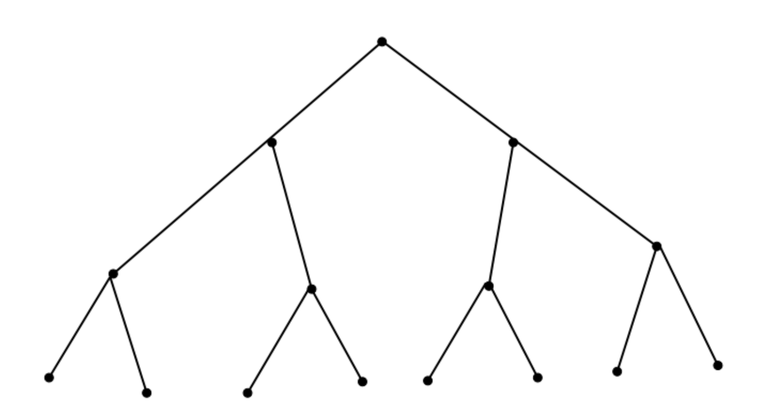
En los árboles con raíz se asume que las direcciones van desde el vértice raíz hacia abajo, por lo que las flechas se pueden eliminar. Si el grado de salida, de un vértice v, $gr^{-}(v)$, en un árbol con raíz es cero (0), al vértice v se le llama **Hoja o vértice terminal**. Por ejemplo, en el árbol con raíz G_2, de la figura anterior, los vértices c, d, g, h y i son hojas. Los demás vértices se llaman internos o nodos de ramificación. El camino desde el vértice raíz hasta el vértice e es de longitud 2 y se dice que e está en el nivel dos (2) y asi sucesivamente. Al vértice b se le llama **Padre** de e y al vértice e se le llama **Hijo** de b. A los vértices h y i se les llama Descendientes de los vértices f, b y r, mientras que a los vértices f, b y r se les llama **Antecesores** de h y i. Dos vértices con el mismo padre se llaman **Hermanos**. Por ejemplo, los vértices h y i son hermanos porque tienen el mismo padre, f.

Definición

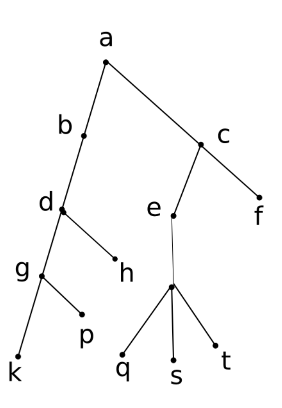
Sea $T = (V, A)$ un árbol con raíz y $n \in \mathbb{Z}^+$. Decimos que T es un Árbol n-ario, si el grado de salida, $gr^-(v)$, de cualquier vértice interno v es n. Si $n = 2$ se dice que el árbol es un **Árbol binario.**

Ejemplo

La siguiente figura es un árbol binario.



1. Considere el árbol siguiente y responda las preguntas:



a. ¿Cuáles vértices representan las hojas?
b. ¿Cuál es el vértice raíz?
c. ¿Cuál vértice es el padre de g?
d. ¿Cuáles vértices son los descendientes de g?
e. ¿Cuáles vértices son hermanos de s?
f. ¿Cuál es el número de nivel del vértice f?
g. ¿Cuáles vértices tienen número de nivel 4?
h. ¿Cuál es la altura del árbol?

2. Sea $T = (V, A)$ un árbol con raíz ordenado por un sistema universal de direcciones.
   a. Si el vértice v de T tiene dirección 2.1.3.6, ¿cuál es el menor número de hermanos que debe tener v?.
   b. Para el vértice v del apartado a., hállese la dirección de su padre.
   c. ¿Cuántos antecesores tiene el vértice v del apartado a.

d. ¿Qué otras direcciones debe haber en el sistema con la presencia de v en T?.

e. Escriba la expresión $(w + x - y)/(\pi * z^3)$ en notación polaca, utilizando un árbol con raíz.

f. ¿Cuál es el valor de la expresión (en notación polaca): $a - b * c + d * e * f$, si $a = c = d = e = 2,\ b = f = 4$?

Contenido

En realidad, podemos definir un árbol de decisión de muchas maneras. Vamos a decir que un **Árbol de decisión** es un sistema que clasifica un conjunto de entrada en una serie de clases predefinidas utilizando un conjunto de preguntas secuenciales. Cada pregunta se relaciona con una variable de entrada.
Los árboles de decisión se pueden usar para desarrollar estarategias óptimas cuando el que toma las decisiones se les presentan casos como:

a. Un conjunto de alternativas de decisión.
b. Incertidumbre o eventos futuros con riesgos.

Necesariamente un análisis de decisiones bueno debe incluir un estudio de riesgo.
Los componentes y estructura de los árboles de decisión son:

a. **Alternativas de decisión** en cada punto de decisión.
b. Los **Eventos (Estados de la naturaleza)** que pueden ocurrir como resultado de cada alternativa de decisión.
c. Las **Probabilidades** de que ocurran los eventos posibles.
d. Los **Resultados (Pagos)** de las posibles interacciones entre las alternativas de decisión y los eventos.

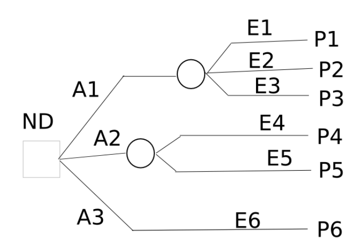
Los árboles de decisión se componen de :

a. **Ramas:** se representan con líneas.

b. **Nodos de decisión:** se representan con □.
c. **Nodos de incertidumbre:** se representan por ○.

Ejemplo

Árbol de decisión



Contenido

En una sección anterior estuvimos tratando ligeramente de funciones y algoritmos recursivos. Es decir, un concepto donde un objeto se define en términos de versiones anteriores del mismo objeto. Así, podemos tener el objeto $a_n, \;\; n \geq 0$ definido en función de $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$. La expresión matemática que formaliza este concepto es lo que se llama un relación de recurrencia o ecuación de diferencias.

Definición

Una **relación de recurrencia** para la sucesión $a_0,\, a_1,\, a_2, \ldots$ es una ecuación que expresa a_n en términos de algunos predecesores $a_0,\, a_1,\, a_2, \ldots, a_{n-1}$. Los valores dados en forma explícita para un número finito de predecesores se les llama **condiciones iniciales** para la sucesión $a_0,\, a_1,\, a_2, \ldots$.

Ejemplo

Consideremos la sucesión $3,\ 8,\ 13,\ 18,\ 23, \ldots$. Si observamos y analizamos esta sucesión, nos damos cuenta que ésta puede ser escrita como

$$a_n = a_{n-1} + 5, \ \ n \geq 1, \quad \text{y} \quad a_0 = 3 \ \text{ como condición inicial.}$$

Ejemplo

Consideremos la sucesión $1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13, \ldots$. La relación de recurrencia de esta sucesión viene dada por

$$a_n = a_{n-1} + a_{n-2}, \ \ n \geq 3,$$

con condiciones iniciales

$$a_1 = 1 \text{ y } a_2 = 1.$$

Esta sucesión se conoce con el nombre de *sucesión de Fibonacci*.

Definición

Solución de una relación de recurrencia es una sucesión $a_0, a_1, a_2, \dots$, cuyos términos son generados por la fórmula explicíta que define el término general (a_n) de la relación de recurrencia.
Existen varios métodos para resolver relaciones de recurrencia, de los cuales estudiaremos el de **iteraciónes** y un método para dar solución a relaciones de recurrencia homogéneas lineales con coeficientes constantes.

Para resolver la relación de recurrencia

$$a_n = a_{n-1} + 5, \tag{6}$$

sujeta a la condición inicial

$$a_0 = 3,$$

mediante el método de iteraciones, se procede de la siguiente manera: Se sustituye n por $n-1$ en (6) para obtener la ecuación

$$a_{n-1} = a_{n-2} + 5, \tag{7}$$

Si ahora sustituimos la ecuación (7) en (6), obtenemos la ecuación

$$a_n = a_{n-2} + 5 + 5 = a_{n-2} + 2 \,.\, 5, \tag{8}$$

Sustituyendo n por $n-2$ en (6) y luego, sustituir la expresión resultante en (8) para obtener

$$a_n = a_{n-3} + 5 + 2\,.\,5 = a_{n-3} + 3\,.\,5 \qquad (9)$$

Si se continua el proceso, llegamos a la fórmula general

$$a_n = a_{n-k} + k\,.\,5.$$

Haciendo $k = n$ en la ecuación anterior, se tiene

$$a_n = a_0 + n\,.\,5.$$

Como $a_0 = 3$, obtenemos la fórmula explícita

$$a_n = 3 + 5\,n,$$

como solución de la relación de recurrencia (6).

Ejemplo

Resolver la relación de recurrencia

$$a_n = 2\,a_{n-1},$$

sujeta a condición inicial

$$a_0 = 1,$$

mediante iteraciones.

Solución:

$$a_n = 2\,a_{n-1} = 2\,(2\,a_{n-2}) = 2\,.\,2\,(2\,a_{n-3}) = 2^k\,a_{n-k}.$$

Haciendo $k = n$, se obtiene

$$a_n = 2^n\,a_0.$$

Como $a_0 = 1$, se obtiene la solución mediante la fórmula explícita

$$a_n = 2^n.$$

Ejemplo

Resolver la relación de recurrencia

$$a_n = 2\,a_{n-1} + 1,$$

sujeta a condición inicial

$$a_1 = 1,$$

mediante iteraciones.

Solución:

$$
\begin{aligned}
a_n &= 2\,a_{n-1} + 1 \\
&= 2\,(2\,a_{n-2} + 1) + 1 \\
&= 2^2\,a_{n-2} + 2 + 1 \\
&= 2^2\,(2\,a_{n-3} + 1) + 2 + 1 \\
&= 2^3\,a_{n-3} + 2^2 + 2 + 1 \\
&\vdots \\
&= 2^{n-1}\,a_1 + 2^{n-2} + 2^{n-3} + \cdots + 2 + 1 \\
&= 2^{n-1} + 2^{n-2} + 2^{n-3} + \cdots + 2 + 1 \\
&= 2^n - 1.
\end{aligned}
$$

Contenido

Definición

Sea $k \in \mathbb{N}$. **Una relación de recurrencia homogénea lineal de orden k con coeficientes constantes** tiene la forma

$$c_0\, a_n + c_1\, a_{n-1} + c_2\, a_{n-2} + c_3\, a_{n-3} + \cdots + c_k\, a_{n-k} = f(n), \quad c_k \neq 0, \;\; n \geq k.$$

Si se ofrecen las condiciones iniciales

$$a_0 = p_0,\; a_1 = p_1,\; a_2 = p_2, \ldots, a_{k-1} = p_{k-1},$$

se define la sucesión $a_0,\; a_1,\; a_2, \ldots.$

Si $f(n) = 0$, la relación se le llama **Homogénea**, en caso contrario, se dice **No homogénea.**

Ejemplo

Las relaciones de recurrencia

$$a_n = 2\, a_{n-1} \text{ y } a_n = a_{n-1} + a_{n-2}$$

son homogéneas lineales con coeficientes constantes, de primer y segundo orden, respectivamente.
La relación de recurrencia

$$a_n = 5\, a_{n-1}\, a_{n-2}$$

no es homogénea lineal con coeficientes constantes, porque en una relación de recurrencia homogénea lineal, los términos deben ser de forma $c\, a_k$. La relación dada se llama *no lineal*.

De forma similar, la relación de recurrencia

$$a_n = a_{n-1} + 2n$$

no es homogénea lineal con coeficientes constantes, porque el término $3n$ la hace no homogénea.
La relación de recurrencia

$$a_n = 3\,n\,a_{n-1}$$

no es de coeficientes constantes, porque $3n$ no es constante.

Contenido

Relaciones de recurrencia homogéneas lineales de segundo orden

Las relaciones homogéneas de orden dos tienen la forma:

$$c_0\, a_n + c_1\, a_{n-1} + c_2\, a_{n-2} = 0, \quad n \geq 0$$

Suponga que la solución de esta ecuación tiene la forma

$$a_n = c\, t^n, \quad c \neq 0, \quad t \neq 0.$$

Sustituyendo en $c_0\, a_n + c_1\, a_{n-1} + c_2\, a_{n-2} = 0$ se obtiene

$$c_0\, c\, t^n + c_1\, c\, t^{n-1} + c_2\, c\, t^{n-2} = 0.$$

Simplificando, tenemos la ecuación cuadrática

$$c_0\, t^2 + c_1\, t + c_2 = 0,$$

llamada *Ecuación característica*. Las raices pueden ser: reales diferentes o reales e iguales o complejas conjugadas.

Ejemplo

Resolver la relación $a_n = -a_{n-1} + 6a_{n-2}, \;\; n \geq 2, \;\; a_0 = 1, \;\; a_2 = 2$.

Solución

Si $a_n = c\,t^n, \;\; c, t \neq 0$, se tiene que la ecuación característica es

$$t^2 + t - 6 = 0.$$

Las raices de esta ecuación son:

$$t_1 = 2, \;\; t_2 = -3.$$

Luego, las soluciones de la ecuación son:

$$a_n = 2^n, \;\; a_n = (-3)^n.$$

Teorema

Relaciones de recurrencia homogéneas lineales de segundo orden

Consideremos la relación de recurrencia homogénea lineal con coeficientes constantes de orden dos:

$$c_0\, a_n = c_1\, a_{n-1} + c_2\, a_{n-2}. \tag{10}$$

Si U y V son soluciones de (10), existen dos constantes d_1 y d_2 tales que $S = d_1\, U + d_2\, V$ en una solución de (10).
Si r es una raíz de la ecuación

$$c_0\, t^2 - c_1\, t - c_2 = 0 \quad \text{(ecuación característica)}, \tag{11}$$

entonces $r^n, \;\; n = 0,\, 1,\, 2, \ldots,$ es una solución de (10). Sean $a_0 = p_0$ y $a_1 = p_1$ condiciones iniciales y supongamos que r_1 y r_2 son raíces

de (11), siendo $r_1 \neq r_2$. Entonces existen constantes d_1 y d_2 tales que
$a_n = d_1\, r_1^n + d_2\, r_2^n, \;\; n = 0,\, 1,\, 2, \ldots .$
Si $r = r_1 = r_2$, existen constantes d_1 y d_2 tales que

$$a_n = d_1\, r^n + d_2\, n\, r^n, \;\; n = 0,\, 1,\, 2, \ldots .$$

Demostración

Dejamos la demostración como ejercicio para los estudiantes.

Ejemplo

Supongamos que se desea resolver la relación de recurrencia

Relaciones de recurrencia homogéneas lineales de segundo orden

$$a_n = 7\,a_{n-1} - 12\,a_{n-2}, \qquad (12)$$

sujeta a las condiciones iniciales $a_0 = 2$ y $a_1 = 10$.
Haciendo $a_n = t^n$, se tiene que

$$t^n - 7\,t^{n-1} + 12\,t^{n-2} = 0.$$

Dividiendo por t^{n-2}, obtenemos

$$t^2 - 7\,t + 12 = 0 \quad \text{(ecuación característica).}$$

Las raíces de la ec. característica son $S_1 = 3$ y $S_2 = 4$. Luego,

$$U_n = 3^n \text{ y } V_n = 4^n$$

son soluciones de (12). Según el teorema (866), se tiene que

$$S_n = d_1\, U_n + d_2\, V_n$$

es también una solución.
Utilizando las condiciones iniciales, tenemos el sistema

$$\begin{aligned} 2 &= S_0 = d_1\,3^0 + d_2\,4^0 = d_1 + d_2 \\ 10 &= S_1 = d_1\,3^1 + d_2\,4^1 = 3\,d_1 + 4\,d_2 \end{aligned}$$

Resolviendo este sistema se obtiene la solución

$$d_1 = -2 \text{ y } d_2 = 4.$$

Por tanto, la solución de la relación de recurrencia es

$$a_n = S_n = -2\,.\,3^n + 4\,.\,4^n.$$

1. Encuentre la relación de recurrencia, con condición inicial, que determine la serie geométrica dada.
   a. $2,\ 10,\ 50,\ 250, \ldots$
   b. $1,\ 1/3,\ 1/9,\ 1/27, \ldots$
   c. $6,\ -18,\ 54,\ -162, \ldots$
   d. $-3,\ 15,\ -75,\ 375, \ldots$
2. Halle la solución general de las relaciones de recurrencia.
   a. $a_n - 1.5a_{n-1} = 0,\ \ n \geq 1,\ \ a_0 = 2$
   b. $3a_n - 4a_{n-1} = 0,\ \ n \geq 1,\ \ a_0 = 5$
   c. $2a_n - 3a_{n-1} = 0,\ \ n \geq 1,\ \ a_4 = 81$
3. Si $a_n,\ \ n \geq 0$ es la solución de la relación de recurrencia $a_n - c\, a_{n-1} = 0,\ \ a_3 = 153/49,\ \ a_5 = 1377/2401$?. ¿ Qué valor tiene c?.

4. Halle a_{10}, si $a_n^3 = 7a_{n-1}^3, \;\; n \geq 1, \;\; a_0 = 3$.
5. Resuelva la relaciń de recurrencia
   $a_{n+2} = a_{n+1} + a_n, \;\; n \geq 0, \;\; a_0 = 0, \;\; a_1 = 1$
6. Resuelva las siguientes relaciones de recurrencia.
   a. $a_n - 5a_{n-1} - 6a_{n-2} = 0, \;\; n \geq 2, \;\; a_0 = 1, \;\; a_1 = 3$
   b. $3a_n - 2a_{n-1} - a_{n-2} = 0, \;\; n \geq 2, \;\; a_0 = 7, \;\; a_1 = 3$
   c. $a_n + a_{n-2} = 0, \;\; n \geq 2, \;\; a_0 = 0, \;\; a_1 = 3$
   d. $a_n - 6a_{n-1} + 9a_{n-2} = 0, \;\; n \geq 2, \;\; a_0 = 5, \;\; a_1 = 12$
   e. $a_n = 7a_{n-1} - 10a_{n-2}, \;\; n \geq 2, \;\; a_0 = 3, \;\; a_1 = 15$

Contenido

Definición

Un **Algoritmo** es un conjunto finito de pasos que conduce a la solución de un problema. Es decir, una secuencia de instrucciones que representan un modelo de solución para determinados tipos de problemas. Los algoritmos son completamente independientes de los lenguajes de programación utilizados para su implementación.
Por ejemplo, un programa de computadoras es un conjunto de instrucciones ordenadas y codificadas en un lenguaje de programación de tal manera que representan los pasos de un algoritmo para ser ejecutado en un computador.
Los algoritmos los podemos clasificar en cuatro grandes grupos:

a. **Computacionales:** son aquellos que pueden ser ejecutados en un computador.
b. **No computacionales:** son aquellos que no requieren de computador para ser ejecutados.
c. **Cualitativos:** son aquellos que no involucran cálculo numérico en sus pasos.
d. **Cuantitativos:** son aquellos que involucran cálculo numérico en sus pasos.

Características de un algoritmo

a. **Preciso:** Cada uno de los pasos debe indicar de manera precisa e inequívoca qué se debe hacer.
b. **Finito:** Debe tener un número limitado (finito) de pasos.

c. **Definido:** Debe producir los mismos resultados para las mismas entradas.
d. Puede tener cero (0) o más entradas.
e. Debe producir un resultado.

Todo algoritmo posee las siguientes componentes:

a. Entrada de datos.
b. Proceso
c. Salida de resultados.

Los algoritmos se pueden representar mediante:

a. Diagramas de flujo.

b. Diagramas Nassi-Shneiderman.
c. Pseudocódigos.
d. Lenguaje natural.
e. Fórmulas matemáticas.

Contenido

La **Validez formal** de un algoritmo es un conjunto de técnicas de comprobación formales que permiten demostrar sin un algoritmo funciona correctamente. Un algoritmo funciona correctamente si cumple con las reglas especificadas. Por **Técnicas de comprobación** se entiende como un proceso de inferencia, donde cada sentencia ejecutable posee una regla de inferencia. Para la representación formal, normalmente se usa las **Ternas de Hoare**.

Contenido

Complejidad de un algoritmo

La **Complejidad** de un algoritmo es una función que depende del tamaño de la entrada que utiliza y que determina la cantidad de recursos (tiempo, memoria, espacio, etc.) usada durante la ejecución del mismo. Un algoritmo es más **Eficiente** comparado con otro si consume menos recursos como el tiempo y el espacio de memoria necesarios para ejecutarlo.
La complejidad de un algoritmo se puede clasificar en:

a. **Temporal:** cuando se mide el tiempo de proceso necesario para ejecutarlo.
b. **Espacial:** cuando se mide la cantidad de memoria necesaria para ejecutarlo.

Complejidad de un algoritmo

El tiempo de ejecución de un algoritmo se simboliza generalmente por $T(N)$, donde N es el tamaño de la entrada.

Contenido

Exponentes

Recordemos algunas propiedades de los exponentes.

a. $x^m\, x^n = x^{m+n}$

b. $\dfrac{x^m}{x^n} = x^{m-n}$

c. $(x^m)^n = x^{mn}$

d. $x^n + x^n = 2x^n$

e. $2^n + 2^n = 2^{n+1}$

Logaritmos

En ciencia de la computación, los logaritmos son de base 2 generalmente.

Definición

Sea $a > 0, \ a \neq 1$.
$a^n = b \leftrightarrow \log_a b = n$, donde $\log_a b = n$ se lee "logaritmo base a de b es igual a n "

Algunas propiedades.

a. $\log_a$ es una función creciente, si $a > 1$ y decreciente, si $0 < a < 1$.

b. $\log_a$ es inyectiva. Es decir, si $\log_a x = \log_a y$, entonces $x = y$.

c. $\log_a 1 = 0$

d. $\log_a a = 1$

e. $\log_a a^b = b$

f. $\log_a (x\, y) = \log_a x + \log_a y$

g. $\log_a \left(\dfrac{x}{y}\right) = \log_a x - \log_a y$

h. $\log_a (x^b) = b \, \log_a x$

i. $x^{\log_a y} = y^{\log_a x}$

j. $\log_a b = \dfrac{\log_c b}{\log_c a}, \quad c > 0, \;\; c \neq 1$

El $\log_2$ se representa por lg. Así, $\log_2 x = lgx$. De la misma manera,

$$lg\, lg(x) = lg(lg(x)).$$

Y en general, $lg^{(k)}(x)$ significa k aplicaciones del logaritmo.

Contenido

Una colección de elementos en un orden definido

$$x_1,\ x_2,\ x_3, \ldots, x_n, \ldots$$

es una **sucesión**. Los elementos de una sucesión pueden estar repetidos. El elemento x_1 es el primer término, x_2 es el segundo término y de esa forma el elemento x_n es el término n-ésimo. Si el número de términos de una sucesión es finito, se dice que la sucesión es **finita**; en caso contrario es **infinita**. Una sucesión también se puede definir como una función

$$f : \mathbb{Z}^+ \to \mathbb{R}.$$

Sin embargo, en lugar de escribir $f(n)$ como el valor de la sucesión en n, se escribe x_n y se llama término general de la sucesión. La sucesión $\{x_1, x_2, x_3, \dots\}$ se simboliza por

$$\{x_n\} \quad \text{o} \quad \{x_n\}_{n=1}^{\infty}.$$

También se puede usar paréntesis en lugar de llaves para representar una sucesión y así podemos escribir

$$(x_1, x_2, x_3, \dots).$$

Y simbolizarla por

$$(x_n)_{n=1}^{\infty}.$$

Observe los ejemplos siguientes:

a. $\{2n\}$ $\quad x_n = 2n \quad$ $\{2, 4, 6, \ldots, 2n, \ldots\}$

b. $\left\{\dfrac{n}{n+1}\right\}$ $\quad x_n = \dfrac{n}{n+1} \quad$ $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots, \frac{n}{n+1}, \ldots\right\}$

Cuando se suman los términos de una sucesión $\{x_n\}_{n=1}^{\infty}$, se consigue la expresión

$$x_1 + x_2 + x_3 + \cdots + x_n + \cdots$$

A esta suma se le llama **serie infinita** y se simboliza por

$$\sum_{n=1}^{\infty} x_n.$$

Al símbolo $\sum$ se le llama **sigma.**

Algunas propiedades de la notación sigma

$$\sum_{i=1}^{n} c = nc$$

$$\sum_{i=1}^{n} cx_i = c\sum_{i=1}^{n} x_i$$

$$\sum_{i=1}^{n} (x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$$

$$\sum_{i=1}^{n}(x_i - y_i) = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i$$

Para cambiar el índice en la sumatoria

$$\sum_{i=k}^{n} f(i),$$

se procede de la siguiente manera:
Hacemos $j = i - k$, de donde $i = j + k$.
Si $i = k$ se tiene que $j = 0$.
Si $i = n$ entonces $j = n - k$.

Luego,

$$\sum_{i=k}^{n} f(i) = \sum_{j=0}^{n-k} f(j+k).$$

Ahora consideremos la fórmula

$$\sum_{i=0}^{n} a\, x^{i} = a\left(\frac{x^{n+1}-1}{x-1}\right).$$

Si $a = 1$ y $x = 2$, entonces se tiene

$$\sum_{i=0}^{n} 2^{i} = 2^{n+1} - 1$$

Si $0 < x < 1$ se puede probar que

$$\sum_{i=0}^{n} x^i \leq \frac{1}{1-x}.$$

Cuando $n \to \infty$ se tiene que la suma tiende a

$$\frac{1}{1-x} \quad \text{(serie geométrica de razón < 1).}$$

Es decir,

$$\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}.$$

Por ejemplo, calculemos la suma

$$\sum_{i=1}^{\infty} \frac{i}{4^i}.$$

Escribamos

$$S = \frac{1}{4} + \frac{2}{4^2} + \frac{3}{4^3} + \frac{4}{4^4} + \frac{5}{4^5} + \cdots$$

multiplicando por 4, tenemos

$$4S = 1 + \frac{2}{4} + \frac{3}{4^2} + \frac{4}{4^3} + \frac{5}{4^4} + \cdots$$

Restando ambas ecuaciones se obtiene

$$3S = 1 + \frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + \frac{1}{4^4} + \frac{1}{4^5} + \cdots$$

Luego,

$$S = \frac{4}{9}.$$

Se puede probar que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \approx \frac{n^2}{2}.$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \approx \frac{n^3}{3}.$$

$$\sum_{i=1}^{n} i^k \approx \frac{n^{k+1}}{|k+1|}, \quad k \neq -1.$$

Si $k = -1$, se tiene

$$\sum_{i=1}^{n} i^k = \sum_{i=1}^{n} i^{-1} = \sum_{i=1}^{n} \frac{1}{i} \approx \ln(n) + \gamma,$$

donde $\gamma = 0.577\cdots$ y se le llama *constante de Euler*. A estos números se les llaman armónicos.

Otras fórmulas importantes son:

$$\sum_{i=1}^{n} f(n) = n\, f(n).$$

$$\sum_{i=k}^{n} f(i) = \sum_{i=1}^{n} f(i) - \sum_{i=1}^{k-1} f(i).$$

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n.$$

Supongamos que cada término 2^i representa un bit 1 en binario. Entonces

$$\sum_{i=0}^{n} 2^i = 111\ldots 1.$$

En esta expresión hay $(n+1)$ bits 1. Este número más 1 produce el resultado

$$1000\ldots0 = 2^{n+1}.$$

$$\sum_{i=0}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}.$$

Contenido

La función **Techo** se define como:

$$\lceil\ \rceil : \mathbb{R} \to \mathbb{Z} \quad \ni \quad \lceil x \rceil = \min\{k \in \mathbb{Z} / x \leq k\}.$$

Ejemplos:

$\lceil 3.6 \rceil = \min\{k \in \mathbb{Z}/3.6 \leq k\} = 4$

$\lceil -4.2 \rceil = \min\{k \in \mathbb{Z}/-4.2 \leq k\} = -4$

$\lceil 7 \rceil = \min\{k \in \mathbb{Z}/7 \leq k\} = 7$

propiedades

a. $\forall x \in \mathbb{R}$ se tiene que $\lceil x \rceil \geq x$

b. $x \in \mathbb{Z} \leftrightarrow \lceil x \rceil = x$

Función Techo

c. La función techo es discontinua en $\mathbb{Z}$

La función **Piso** se define como:

$$\lfloor \ \rfloor : \mathbb{R} \to \mathbb{Z} \quad \ni \quad \lfloor x \rfloor = \text{máx}\{k \in \mathbb{Z}/k \leq x\}.$$

Ejemplos:

$\lfloor 3.6 \rfloor = \text{máx}\{k \in \mathbb{Z}/k \leq 3.6\} = 3$

$\lfloor -4.2 \rfloor = \text{máx}\{k \in \mathbb{Z}/k \leq -4.2\} = -5$

$\lfloor 7 \rfloor = \text{máx}\{k \in \mathbb{Z}/k \leq 7\} = 7$

propiedades

a. $\forall x \in \mathbb{R}$ se tiene que $\lfloor x \rfloor \leq x$

b. $x \in \mathbb{Z} \leftrightarrow \lfloor x \rfloor = x$

c. La función piso es discontinua en $\mathbb{Z}$

d. $\lfloor x+n \rfloor = \lfloor x \rfloor + n, \ \ \forall\, n \in \mathbb{Z}, \ \ x \in \mathbb{R}$

e. $\lceil x+n \rceil = \lceil x \rceil + n, \ \ \forall\, n \in \mathbb{Z}, \ \ x \in \mathbb{R}$

f. $\lceil x \rceil = \lfloor x \rfloor + 1, \ \ x \notin \mathbb{Z}$

g. $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}, \ \ n \in \mathbb{Z}, \ \ n$ impar

h. $\left\lceil \frac{n}{2} \right\rceil = \frac{n+1}{2}, \ \ n \in \mathbb{Z}, \ \ n$ impar

1. Determine el valor de:
   a. $\lfloor x \rfloor + \lfloor -x \rfloor$
   b. $\lceil x \rceil + \lceil -x \rceil$
   c. ¿Es cierto que -$\lceil -x \rceil = \lceil x \rceil$?
   d. ¿Es cierto que -$\lfloor -x \rfloor = \lfloor x \rfloor$?
2. Demuestre las siguientes propiedades
   a. $\left\lfloor \frac{n^2}{4} \right\rfloor = \frac{n^2-1}{4}, \quad n \in \mathbb{Z}, \quad n$ impar
   b. $\left\lceil \frac{n^2}{4} \right\rceil = \frac{n^2+3}{4}, \quad n \in \mathbb{Z}, \quad n$ impar

c. $\left\lceil \frac{n}{2} \right\rceil + \left\lfloor \frac{n}{2} \right\rfloor = n$

d. $\lceil x \rceil = -\lfloor -x \rfloor$

La función **Parte entera** se define como:

$$[\ \ ]:\mathbb{R}\to\mathbb{Z}\quad\ni\quad [x]=\begin{cases}\lfloor x\rfloor, & \text{si}\quad x\geq 1\\ 0, & \text{si}\quad -1<x<1\\ \lceil x\rceil, & \text{si}\quad x\leq -1\end{cases}$$

La notación asintótica es una herramienta muy usada cuando necesitamos comparar la tasa de crecimiento de funciones. Se habla de notación asintótica porque nos interesa conocer el comportamiento de las funciones cuando su argumento crece arbitrariamente.

Notación O (O-grande)

$$O(f(n)) = \{g : \mathbb{N} \to \mathbb{R}^+ \,|\, \exists\, c > 0,\ \exists\, n_0 \in \mathbb{N},\ g(n) \leq c\, f(n),\ \forall\, n \geq n_0\}$$

Observemos que $O(f(n))$ es un conjunto de funciones. Sin embargo, es costumbre tomar una representación para la función f. A $f(n)$ se le

llama *cota superior* del conjunto de funciones $g(n)$. Es decir, $O(f(n))$ es el conjunto de funciones que no crecen más rápidamente que $f(n)$.

En lugar de escribir $g(n) \in O(f(n))$, se suele usar la expresión $g(n) = O(f(n))$ y decir "$g(n)$ es o-grande de $f(n)$". Si $g(n)$ no es $O(f(n))$ se escribe $g(n) \notin O(f(n))$.

Otra forma de escribir que $g(n) \in O(f(n))$ es usando el concepto de límite de la siguiente manera:

$$g(n) \in O(f(n)), \text{ si } \lim_{n\to\infty} \frac{g(n)}{f(n)} = c < \infty,$$

donde c puede ser 0.

Si

$$\lim_{n\to\infty} \frac{g(n)}{f(n)} = \infty,$$

decimos que $g(n)$ crece más rápidamente que $f(n)$ y se escribe $g(n) \notin O(f(n))$.

Ejemplo

Sean $f(n) = \frac{1}{2}n^3$ y $g(n) = 21n^2 + 19n + 7$. Probemos que $g(n) \in O(f(n))$.
Si graficamos ambas funciones en un mismo sistema de coordenadas, observamos que para $n \geq 43, \; g(n) < c\, f(n)$, donde $c = 1$ y $n_0 = 43$;

lo que significa que $g(n) \in O(f(n))$. Lo mismo puede ser probado mediante el uso de límite, donde

$$\lim_{n\to\infty} \frac{g(n)}{f(n)} = 0.$$

De la misma forma, tenemos que:

$$17n^3+8n \in O(n^3), \qquad 13n^2+2n+11 \in O(n^3), \qquad 3n^2+7n+78 \in O(n^2).$$

En ocasiones, para calcular el límite es necesario uitlizar la regla de L'Hopital que dice:

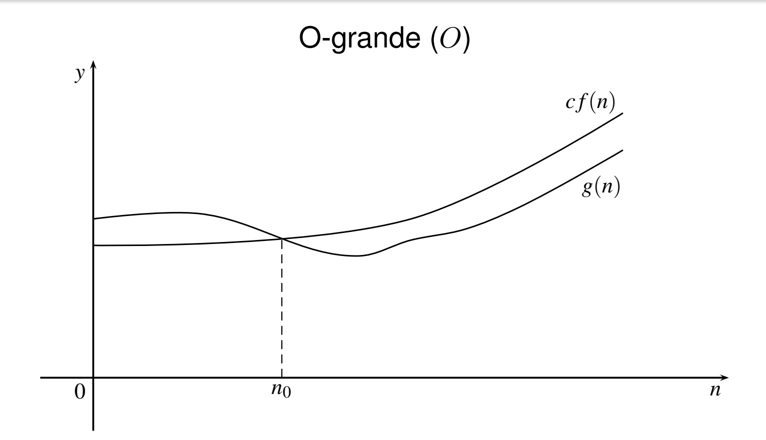
Si $f(n)$ y $g(n)$ son diferenciables con $f'(n)$ y $g'(n)$ como sus derivadas respectivas y si

$$\lim_{n\to\infty} f(n) = \lim_{n\to\infty} g(n) = \infty,$$

entonces

$$\lim_{n\to\infty} \frac{g(n)}{f(n)} = \lim_{n\to\infty} \frac{g'(n)}{f'(n)}.$$

La figura siguiente muestra una imagen de O-grande:


O-grande (O)
y
$cf(n)$
$g(n)$
0
n_0
n

Ejemplo
Sean las funciones $f(n) = n^{3/2}$ y $g(n) = n\, lg\, n$. probemos mediante límite que $g(n) \in O(f(n))$.

$$\begin{aligned}
\lim_{n\to\infty} \frac{g(n)}{f(n)} &= \lim_{n\to\infty} \frac{n\, lg\, n}{n^{3/2}} = \lim_{n\to\infty} \frac{lg\, n}{n^{1/2}} = \lim_{n\to\infty} \frac{\ln\ n}{(\ln\ 2)\, n^{1/2}} \\
&= \left(\frac{1}{\ln\ 2}\right) \lim_{n\to\infty} \frac{\ln\ n}{n^{1/2}} \\
&= \left(\frac{1}{\ln\ 2}\right) \lim_{n\to\infty} \frac{1/n}{1/2\sqrt{n}}, \qquad \text{por L'Hopital} \\
&= \left(\frac{1}{\ln\ 2}\right) \lim_{n\to\infty} \frac{2}{\sqrt{n}} = \left(\frac{1}{\ln\ 2}\right)(0) = 0.
\end{aligned}$$

Luego, $g \in O(f(n))$.

Propiedades de O (O-grande)

a. Reflexiva: $f(n) \in O(f(n))$.

b. Transitiva: Si
$g(n) \in O(f(n))$ y $f(n) \in O(h(n))$, entonces $g(n) \in O(h(n))$.

Otras propiedades de la notación O (O-grande):

Regla de la constante

Sea c una constante cualquiera. Entonces

c. $f(n) + c \in O(f(n))$.

d. $c\,f(n) \in O(f(n))$.

Regla de la suma

e. Si $g_1(n) \in O(f_1(n))$ y $g_2(n) \in O(f_2(n))$, entonces $g_1(n) + g_2(n) \in O(\text{máx}\{f_1(n), f_2(n)\})$.

Regla del producto

f. Si $g_1(n) \in O(f_1(n))$ y $g_2(n) \in O(f_2(n))$, entonces $g_1(n) * g_2(n) \in O(f_1(n) * f_2(n))$,

Notación Ω (Omega)

$$\Omega(f(n)) = \{g : \mathbb{N} \to \mathbb{R}^+ \mid \exists\, c > 0,\, \exists\, n_0 \in \mathbb{N},\, g(n) \geq c\, f(n),\, \forall\, n \geq n_0\}$$

En este caso decimos que $f(n)$ es una *cota inferior* del conjunto de funciones $g(n)$.
La técnica de los límites nos permite definir la notación Ω como:

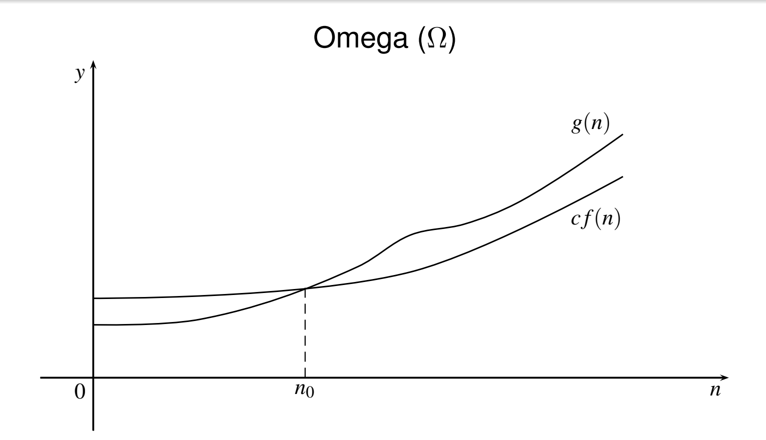
$$g(n) \in \Omega(f(n)), \text{ si } \lim_{n\to\infty} \frac{g(n)}{f(n)} = c > 0,$$

donde c puede ser ∞.
Ejemplo

$$\frac{n^2}{2} \in \Omega(n^2), \qquad 5n^3 + 2n \in \Omega(n^2), \quad \text{pero} \;\; n^2 \notin \Omega(n^3).$$

La figura siguiente muestra una ilustración de la notación Ω.

Omega (Ω)



Propiedades de Ω (Omega)

a. Reflexiva: $f(n) \in \Omega(f(n))$

b. Transitiva: Si
$g(n) \in \Omega(f(n))$ y $f(n) \in \Omega(h(n))$, entonces $g(n) \in \Omega(h(n))$

Otras propiedades de la notación Ω:

Regla de la constante

Sea c una constante cualquiera. Entonces

c. $f(n) + c \in \Omega(f(n))$.

d. $c\,f(n) \in \Omega(f(n))$.

Regla de la suma

e. Si $g_1(n) \in \Omega(f_1(n))$ y $g_2(n) \in \Omega(f_2(n)$, entonces $g_1(n) + g_2(n) \in \Omega(\text{máx}\{f_1(n), f_2(n)\})$.

Regla del producto

f. Si $g_1(n) \in \Omega(f_1(n))$ y $g_2(n) \in \Omega(f_2(n)$, entonces $g_1(n) * g_2(n) \in \Omega(f_1(n) * f_2(n))$.

g. $g(n) \in O(f(n)) \Longleftrightarrow f(n) \in \Omega(g(n))$.

Notación Θ (Theta)

$$\begin{aligned}\Theta(f(n)) &= \{g : \mathbb{N} \to \mathbb{R}^+ \mid \exists\, c_1, c_2 > 0, \exists\, n_0 \in \mathbb{N}, \\ &\quad c_1 f(n) \leq g(n) \leq c_2 f(n), \forall\, n \geq n_0\} \\ &= O(f(n)) \cap \Omega(f(n)).\end{aligned}$$

La técnica de los límites nos permite definir la notación Θ como:

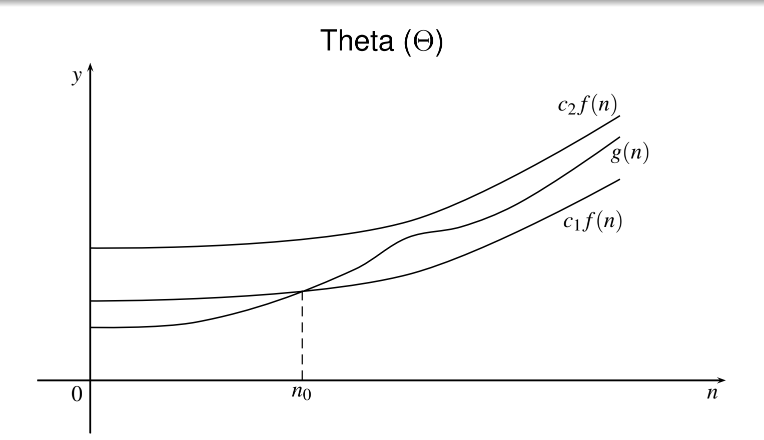
$$g(n) \in \Theta(f(n)), \text{ si } \lim_{n\to\infty} \frac{g(n)}{f(n)} = c, \text{ donde } 0 < c < \infty.$$

Ejemplo

$$5n^2 - n \in \Theta(n^2), \qquad 7n + 2000 \in \Theta(n), \quad \text{pero} \;\; n \notin \Theta(n^2).$$

La figura siguiente es una ilustración de la notación Θ:

Theta (Θ)



Propiedades de Θ (Theta)

a. Reflexiva: $f(n) \in \Theta(f(n))$.

b. Simétrica: $g(n) \in \Theta(f(n)) \Leftrightarrow f(n) \in \Theta(g(n)$.

c. Transitiva: Si
$g(n) \in \Theta(f(n))$ y $f(n) \in \Theta(h(n))$, entonces $g(n) \in \Theta(h(n))$.

Esto significa que la notación Θ define una relación de equivalencia sobre las funciones. El conjunto $\Theta(f)$ representa una clase de equivalencia, al cual se le llama *clase complejidad*.

Otras propiedades de la notación Θ:

Regla de la constante

Sea c una constante cualquiera. Entonces

d. $f(n) + c \in \Theta(f(n))$.

e. $c\, f(n) \in \Theta(f(n))$.

Regla de la suma

f. Si $g_1(n) \in \Theta(f_1(n))$ y $g_2(n) \in \Theta(f_2(n))$, entonces $g_1(n) + g_2(n) \in \Theta(\text{máx}\{f_1(n), f_2(n)\})$.

Regla del producto

g. Si $g_1(n) \in \Theta(f_1(n))$ y $g_2(n) \in \Theta(f_2(n))$, entonces $g_1(n) * g_2(n) \in \Theta(f_1(n) * f_2(n))$.

Es costumbre indicar la clase de complejidad de un algoritmo, escogiendo la función más simple dentro de la clase. Si la función de complejidad de un algoritmo viene dada por $T(n) = n^3 + 2n + 27$, se dice que la complejidad del algoritmo es de orden $\Theta(n^3)$ o está en $\Theta(n^3)$. Cuando $f(n) \in \Theta(n)$, se dice que $f(n)$ es lineal; cuando $f(n) \in \Theta(n^2)$, se dice que $f(n)$ es cuadrática y así sucesivamente.

Notación o (o-pequeña)

$$\begin{aligned} o(f(n)) &= \{g : \mathbb{N} \to \mathbb{R}^+ \,|\, \exists\, c > 0,\, \exists\, n_0 \in \mathbb{N},\, g(n) < c\, f(n),\, \forall\, n \geq n_0\} \\ &= O(f(n)) - \Theta(f(n)) \end{aligned}$$

El uso de los límites nos permite definir la notación o como:

$$g \in o(f), \text{ si } \lim_{n\to\infty} \frac{g(n)}{f(n)} = 0.$$

Notación ω (omega)

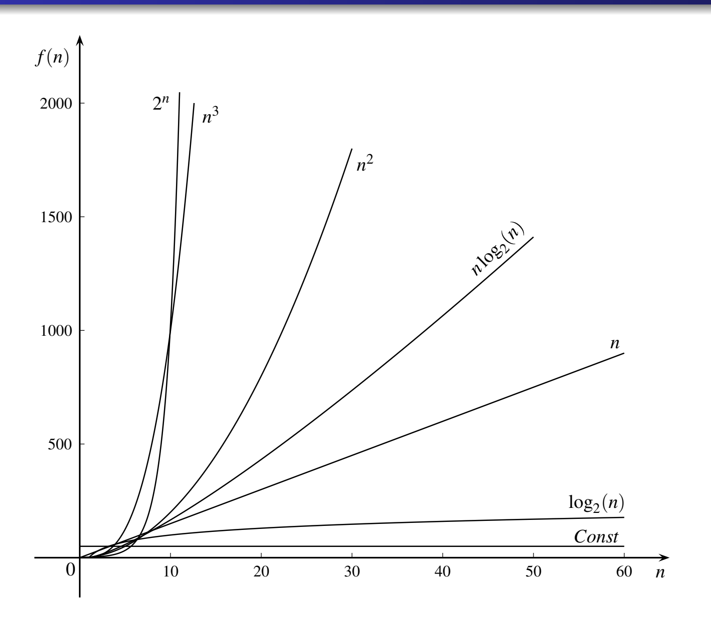
$$\begin{aligned}\omega(f(n)) &= \{g : \mathbb{N} \to \mathbb{R}^+ \mid \exists\, c > 0,\, \exists\, n_0 \in \mathbb{N},\, g(n) > c\, f(n),\, \forall\, n \geq n_0\} \\ &= \Omega(f(n)) - \Theta(f(n))\end{aligned}$$

El uso de los límites nos permite definir la notación ω como:

$$g(n) \in \omega(f(n)), \text{ si } \lim_{n\to\infty} \frac{g(n)}{f(n)} = \infty.$$

La figura siguiente muestra una comparación de la tasa de crecimiento de funciones comunes en el análisis de complejidad algorítmica.

Comparación tasa de crecimiento de funciones comunes


$f(n)$
2000
1500
1000
500
0
2^n
n^3
n^2
$n\log_2(n)$
n
$\log_2(n)$
Const
10
20
30
40
50
60
n

Conceptos y definiciones

En la ciencia de la computación juegan un papel importante las cadenas o palabras (conjunto de símbolos o caracteres). Por ejemplo, un programa de computadora es un conjunto de sucesiones finitas de caracteres, que necesitan ser manipuladas algebraicamente a través de reglas y/o procedimientos definidos para tales fines. En este sentido, los lenguajes formales representan un subcampo importante en el estudio de ciencia de la computación. El estudio de la teoría de lenguajes formales se inicia a mediado de la decada de 1950.

Definición

Se llama **Alfabeto o vocabulario** a un conjunto finito no vacío de símbolos indivisibles. Se representa por

$$\sum .$$

Ejemplos

$$\sum_{1} = \{a, b\}, \qquad \sum_{2} = \{0, 1\}, \qquad \sum_{3} = \{\text{begin, end, for}\}.$$

El conjunto $A = \{a, b, c, ab, bb, abc\}$ no es un alfabeto, porque en un alfabeto no puede haber elementos que resulten de la yuxtaposición de otros elementos básicos de alfabeto.

Si $\sum$ es un alfabeto, definimos,

$$\sum^{2} = \left\{ xy \,|\, x, y \in \sum \right\}, \qquad \sum^{3} = \left\{ xy \,|\, x \in \sum, y \in \sum^{2} \right\}.$$

A los elementos de $\sum^{2}$ y $\sum^{3}$ se les llama **Cadenas o palabras** de longitud 2 y 3, respectivamente. De forma recursiva definimos

$$\sum^{n+1} = \left\{ xy \,|\, x \in \sum, y \in \sum^{n} \right\}, \;\; n \geq 1,$$

donde $\sum^{1} = \sum$.

La cadena o palabra vacía (nula) es la que no está formada por algún símbolo del alfabeto y se representa por λ. Así que

$$\sum^0 = \{\lambda\}.$$

Es importante aclarar que la cadena vacía no es el espacio en blanco.

Recordemos que $\emptyset \subseteq \sum$. También debemos saber que $\{\lambda\} \not\subseteq \sum$, puesto que $\lambda \notin \sum$. De la misma manera, $\{\lambda\} \neq \emptyset$, ya que $|\{\lambda\}| = 1, \quad |\emptyset| = 0$.
Ahora definimos

$$\sum^* = \bigcup_{n=0}^{\infty} \sum^n \ \text{ y } \ \sum^+ = \bigcup_{n=1}^{\infty} \sum^n .$$

Por ejemplo, si consideramos el alfabeto

$$\sum_2 = \{0, 1\},$$

tenemos que

$$\sum_2^* = \{\lambda, 0, 1, 11, 001, 1101, 111111, 00000, \dots\}$$

y

$$\sum_2^+ = \{0, 1, 11, 001, 1101, 111111, 00000, \dots\}.$$

Observemos que

$$\sum^* = \sum^+ \cup \{\lambda\}.$$

A los elementos de

$$\sum^* \text{ y } \sum^+$$

se les llama **Cadenas o palabras** sobre el alfabeto $\sum$. A $\sum^*$ se le llama con frecuencia **Universo** sobre el alfabeto $\sum$.

El alfabeto $\sum \subset \sum^*$. El conjunto $\sum^*$ es infinito contable. Es decir, su cardinal es infinito.

Si $n \in \mathbb{Z}^+$, se tiene que $|\sum^n| = |\sum|^n$. Sea $n \in \mathbb{Z}^+$ y $w,\ v \in \sum^n$, tales que $w = x_1x_2\cdots x_n$ y $v = y_1y_2\cdots y_n$, siendo $x_i, y_i \in \sum,\ 1 \leq i \leq n$. Decimos que $w = v$, si $x_i = y_i,\ 1 \leq i \leq n$.

La **Longitud** de una cadena $w \in \sum^*, w \neq \lambda, w = x_1x_2\cdots x_n$ se define como el número de símbolos que contiene w y se representa por $|w|$.

En este caso, $|w| = n$. La longitud de la cadena vacía λ es $|\lambda| = 0$. Es claro que toda cadena de $\sum^{+}$ es de longitud positiva.

Por ejemplo, la palabra $w = 1000110101$ sobre el alfabeto $\sum_2$ tiene longitud $|w| = 10$.

Definición

Sean $x, y \in \sum^*$. La **Concatenación** de x y y es otra palabra de $\sum^*$ definida como $x.y = x\,y$. Es decir, los símbolos de x seguidos de los símbolos de y. Por ejemplo, si $\sum = \{a, b\}$ y $x = abbaabbb$ y $y = bbbaabaaa$ son palabras de $\sum^*$, entonces tenemos que $x\,y = abbaabbbbbbaabaaa$.

Propiedades de la concatenación

1. Es una operación cerrada sobre $\sum^*$.
2. Es asociativa : $(x\,y)\,z = x\,(y\,z), \quad \forall x, y, z \in \sum^*$
3. Elemento neutro λ : $\lambda\,x = x = x\,\lambda.$
4. $|x\,y| = |x| + |y|, \quad \forall x, y \in \sum^*$
5. No es conmutativa

Sea $x \in \sum^*$, $k \in \mathbb{Z}^+$. La **Potencia** x^k se define como la concatenación de x consigo misma k veces. Es decir,

$$x^k = \underbrace{x\,x\,\cdots\,x}_{k \text{ veces}}.$$

Por ejemplo, Si $x = abba$ entonces $x^2 = x\,x = abbaabba$ y $x^3 = x\,x\,x = abbaabbaabba$.

propiedades de la potencia

Sean $m, n \in \mathbb{Z}^+$.

1. $x^1 = x$
2. $x^{m+n} = x^m\,x^n$.

Potencias de una palabra

3. $|x^m| = m\,|x|$
4. $x^0 = \lambda$
5. $|x^{m+n}| = (m+n)|x| = m\,|x| + n\,|x| = |x^m| + |x^n|$

Inversa o reflexión de una palabra

Sea $x \in \sum^*$. La **Inversa** de la palabra x, representada por x^{-1} es otra palabra de $\sum^*$ que contiene los mismos símbolos de x, pero dispuestos en orden inverso.

Por ejemplo, si $x = abab$ entonces $x^{-1} = baba$.

Propiedades

1. $|x| = |x^{-1}|$
2. $\lambda^{-1} = \lambda$

Definición

Si $x\,y = w$, a x se le llama **Prefijo** de w y a y se le llama **Sufijo** de w. Puesto que $\lambda\,w = w = w\,\lambda$, decimos que λ es prefijo y sufijo trivial de cualquier palabra. De la misma forma decimos que w es prefijo y sufijo trivial de si misma.

Propiedades

1. Si x es prefijo de w, entonces $|x| \leq |w|$.
2. Si y es sufijo de w, entonces $|y| \leq |w|$.

Ejercicio

1. Si x es prefijo de w y y es sufijo de w con $x = y$, entonces ¿qué puede decirse de $x = y = w$?.

Contenido

Definición

Sea $\sum$ un alfabeto. Un **Lenguaje** es cualquier subconjunto L de $\sum^*$ (Universo). Es decir, $L \subset \sum^*$.

Ejemplos

El conjunto $L_\emptyset = \emptyset$ es llamado el **Lenguaje vacío** y $|L_\emptyset| = 0$.

El conjunto $L_\lambda = \{\lambda\}$ es el lenguaje que sólo contiene la palabra vacía y $|L_\lambda| = 1$.

A estos lenguajes se les llama **Triviales** y son independientes del alfabeto. Por tanto, son lenguajes sobre cualquier alfabeto.

Ejemplo

Sea $\sum = \{a, b\}$. Los conjuntos siguientes representan lenguajes:

1. $L_1 = \{\lambda, a, b\}$.
2. $L_2 = \{x^n\, y^n \,|\, x, y \in \sum^*,\, n \in \mathbb{N}\}$.
3. $L_3 = \{x\, x^{-1} \,|\, x \in \sum^*\}$ (Palíndromos)
4. $L_4 = \{x^{n^2} \,|\, x \in \sum^*,\, n \in \mathbb{Z}^+\}$
5. $L_5 = \{x \,\big|\, |x| = 5,\, x \in \sum^*\}$
6. $L_6 = \{x \,|\, x$ no contenga un número par de $a's\}$

Definición

Un lenguaje $L \subset \sum^*$ se dice **Finito** si $|L|$ es un número natural. Es decir, si $|L| < \infty$.

Sean L, L_1, L_2, L_3 lenguajes de $\sum^*$.

Unión

$$L_1 \cup L_2 = \{w \,|\, w \in L_1 \text{ o } w \in L_2\}.$$

Propiedades

1. Es conmutativa: $L_1 \cup L_2 = L_2 \cup L_1$
2. Es asociativa: $(L_1 \cup L_2) \cup L_3 = L_1 \cup (L_2 \cup L_3)$
3. Idempotencia: $L \cup L = L$
4. $L \cup \emptyset = \emptyset \cup L = L$
5. $L \cup \sum^* = \sum^* \cup L = \sum^*$

Intersección

$$L_1 \cap L_2 = \{w \,|\, w \in L_1 \text{ y } w \in L_2\}.$$

Propiedades

1. Es conmutativa: $L_1 \cap L_2 = L_2 \cap L_1$
2. Es asociativa: $(L_1 \cap L_2) \cap L_3 = L_1 \cap (L_2 \cap L_3)$
3. Idempotencia: $L \cap L = L$
4. $L \cap \emptyset = \emptyset \cap L = \emptyset$
5. $L \cap \sum^* = \sum^* \cap L = L$

Complemento

$$L^c = \{w \,|\, w \in \sum^* \text{ y } w \notin L\}.$$

Propiedades

1. $(L_1 \cup L_2)^c = L_1^c \cap L_2^c$ (Ley de D'Morgan)
2. $(L_1 \cap L_2)^c = L_1^c \cup L_2^c$ (Ley de D'Morgan)

Utilizando las operaciones que se acaban de definir, se puede probar que $B = (\sum^*, \cup, \cap, ^c)$ forma una álgebra booleana.

Diferencia

$$L_1 - L_2 = \{w \,|\, w \in L_1 \ \text{ y } \ w \notin L_2\}.$$

Propiedades

1. $L_1^c = \sum^* - L_1$
2. $L_1 - L_2 = L_1 \cap L_2^c$

Concatenación

$$L_1\, L_2 = L_1\, .\, L_2 = \{w \,|\, w = w_1\, w_2,\ w_1 \in L_1,\ w_2 \in L_2\}.$$

Propiedades

1. No conmutativa
2. $L\, .\, \emptyset = \emptyset\, .\, L = L$
3. $L\, .\, \{\lambda\} = \{\lambda\}\, .\, L = L$

Potencia

Sea $k \in \mathbb{Z}^+$.

$$L^k = \underbrace{L\,L\,\ldots\,L}_{k\text{ veces}}$$

Propiedades

1. $L^0 = \{\lambda\}$
2. Recursividad: $L^{k+1} = L\,L^k = L^k\,L$

Clausura positiva

$$L^{+} = \bigcup_{i=1}^{\infty} L^{i} = L^{1} \cup L^{2} \cup L^{3} \ldots .$$

Clausura de Kleene

$$L^{*} = \bigcup_{i=0}^{\infty} L^{i} = L^{0} \cup L^{1} \cup L^{2} \cup L^{3} \ldots .$$

Propiedades

1. $L^{+} = L^{*} - \{\lambda\}$
2. $\sum^{*} = \bigcup_{i=0}^{\infty} \sum^{i}$

Inverso o reflexión

$$L^{-1} = \{w^{-1} \,|\, w \in L\}$$

Recordatorio sobre conceptos previos

Sea $\sum$ un alfabeto. Recordemos que una **Relación binaria** sobre $\sum^*$ es cualquier conjunto $R \subset \sum^* \times \sum^*$. Los elementos de R se representan como (x, y) o $x \Rightarrow y$ o $x \, R \, y$.

Sean R y S dos relaciones sobre $\sum^*$. Entonces

$$\begin{aligned} R\,S &= \left\{(x,y)\,|\,\exists z \in \sum^* : x\,R\,z, \quad z\,S\,y\right\} \\ R^0 &= \left\{(x,x)\,|\,x \in \sum^*\right\} \quad \text{(identidad)} \\ R^{n+1} &= R\,R^n \end{aligned}$$

Ahora definimos,

$$R^* = \bigcup_{n=0}^{\infty} R^n$$

$$R^+ = \bigcup_{n=1}^{\infty} R^n.$$

Es decir, $x\,R^*\,y$ o $x \overset{*}{\Rightarrow} y$, si $x = y$ o $\exists z_1, z_2, \ldots, z_n \in \sum^*$ tales que $x\,R\,z_1, z_1\,R\,z_2, \ldots, z_{n-1},\ z_n\,R\,y$.

Sea $\sum$ un alfabeto. Recordemos que una relación $R \subset \sum^* \times \sum^*$ es de **equivalencia** si es:

a. Reflexiva : $\forall x\ : x\,R\,x$. Es decir que $R^0 \subset R$.

b. Simétrica : si $\forall x, y : x\,R\,y\ \wedge\ y\,R\,x$

c. Transitiva : si $x\,R\,y, y\,R\,z \rightarrow x\,R\,z$

En este sentido tenemos que R^* es refleviva y transitiva. A R^* se le llama **Clausura reflexiva y transitiva** de R. A R^+ se le llama **Clausura transitiva** de R. Si R es reflexiva, entonces R^+ es también reflexiva. R^+ y R^* son simétricas, si R es simétrica.

Contenido

Definición (Producción)

Sea $\sum$ un alfabeto. Una **Producción o regla** definida sobre el alfabeto $\sum$ es un par ordenado de palabras (x, y), donde $x, y \in \sum^*$. Se dice que x es la **parte izquierda** de la producción y y es la **parte derecha** de la producción. Las producciones también reciben el nombre de **Reglas de derivación**. Se representan normalmente por $x \to y$ o $x ::= y$.

Definición (Producción compresora)

Decimos que una producción es **Compresora** si la longitud de la parte derecha es menor que la longitud de la parte izquierda.

Definición (Derivación directa)

Sea $\sum$ un alfabeto,

$$P = \left\{ \begin{array}{ccc} x_1 & \rightarrow & y_1 \\ x_2 & \rightarrow & y_2 \\ & \cdots & \\ x_n & \rightarrow & y_n \end{array} \right\}$$

o

$$P = \{x_1 \rightarrow y_1, x_2 \rightarrow y_2, \ldots, x_n \rightarrow y_n\}$$

un conjunto de producciones definidas sobre $\sum$ y $v, w \in \sum^*$. Se dice que v produce directamente a w o que w deriva directamente de v, si existen $\alpha_1, \alpha_2 \in \sum^*$ y una producción $x_i \rightarrow y_i$ tal que $v = \alpha_1\, x_i\, \alpha_2$ y $w = \alpha_1\, y_i\, \alpha_2$. Para decir que v produce directamente a w se escribe

$v \Rightarrow w$. Por ejemplo, si se tiene la palabra $v = 0A1$ y la producción $A \rightarrow B$, entonces se deriva la palabra $w = 0B1$.

De la misma manera, si se tiene las producciones $000 \rightarrow 110$ y $10 \rightarrow 01$, de la palabra 1000 se pueden derivar las palabras $w_1 = 1110$ y $w_2 = 0100$, aplicando la primera y segunda producción, respectivamente.

Definición (Derivación)

Sea $\sum$ un alfabeto, P un conjunto de producciones definidas sobre $\sum$ y $v, w \in \sum^*$. Se dice que v produce a w o que w deriva de v, si existen $w_0, w_1, \ldots, w_m \in \sum^*$ tales que

$$\begin{aligned} v &= w_0 \Rightarrow w_1 \\ & w_1 \Rightarrow w_2 \\ & \ldots \\ & w_{m-1} \Rightarrow w_m = w. \end{aligned}$$

En este caso se usa la notación $v \overset{*}{\Rightarrow} w$. Es decir, w deriva de v cuando se aplica una secuencia de derivaciones directas de un conjunto de producciones. Se define como **Longitud de una derivación** al número de producciones aplicadas.

Definición

Una **Gramática formal** es una cuádrupla

$$G = \left(\sum_N, \sum_T, P, S\right),$$

donde

a. $\sum_N$ es un alfabeto finito de símbolos no terminales o variables.
b. $\sum_T$ es un alfabeto finito de símbolos terminales.
c. P es un conjunto finito de producciones.
d. S es el símbolo de inicio o axioma y pertenece a $\sum_N$.
e. $\sum_N \cap \sum_T = \emptyset, \qquad \sum_N \cup \sum_T = \sum$

Durante el desarrollo de este estudio, utilizaré letras mayúsculas para los símbolos no terminales o variables. Letras minúsculas para los símbolos terminales. Las cadenas de terminales se representarán por las últimas letras del alfabeto en minúsculas. Las cadenas de variables y símbolos terminales se representarán por letras griegas en minúsculas.

Definición

El **Lenguaje generado** por la gramática G se define como

$$L(G) = \{w \,|\, w \in \sum\nolimits_T^*,\ S \overset{*}{\Rightarrow} w\}.$$

Es decir, $w \in L(G)$, si :

a. w sólo contiene símbolos terminales.

b. w puede ser derivado de S.

Decimos que una cadena de símbolos terminales y no terminales α es una **Forma sentencial** si $S \stackrel{*}{\Rightarrow} \alpha$.

Dos gramáticas G_1 y G_2 son **Equivalentes** si $L(G_1) = L(G_2)$.

Definición (Recursividad)

Una **Derivación recursiva** es aquella que tiene la forma $A \stackrel{*}{\Rightarrow} \alpha_1 A \alpha_2$, donde $A \in \sum_N$, $\alpha_1, \alpha_2 \in \sum^*$.

Una gramática $G = (\sum_N, \sum_T, P, S)$ es **Recursiva** si tiene derivaciones recursivas. Es decir, derivaciones del tipo $A \stackrel{*}{\Rightarrow} \alpha_1 A \alpha_2$. Si

$\alpha_1 = \lambda$ se dice que G es recursiva por la izquierda y si $\alpha_2 = \lambda$ se dice que G es recursiva por la derecha.

Si en P hay producciones de la forma $A \to \alpha_1 A \alpha_2$, es claro que G es recursiva.

Teorema

Un lenguaje $L(G)$ es infinito, si y sólo si, G es recursiva.

Ejemplo 1

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum\nolimits_N = \{S\}, \;\; \sum\nolimits_T = \{a, b\}, \;\; P = \{S \to aSb, S \to ab\}.$$

Solución

Si aplicamos la primera producción $n-1$ veces y después la segunda producción , se obtiene

$$S \Rightarrow aSb \Rightarrow aaSbb \Rightarrow a^3Sb^3 \Rightarrow a^{n-1}Sb^{n-1} \Rightarrow a^nb^n.$$

Luego, el lenguaje generado por la gramática G es

$$L(G) = \{a^n\, b^n \,|\, n \geq 1\}.$$

Ejemplo 2

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum\nolimits_N = \{S\}, \ \ \sum\nolimits_T = \{a, b\}, \ \ P = \{S \to \lambda, S \to aS, S \to bS\}.$$

Solución

Si aplicamos la segunda producción n veces y después la primera producción , se obtiene

$$S \Rightarrow aS \Rightarrow aaS \Rightarrow \cdots \Rightarrow a^n.$$

Si aplicamos la tercera producción m veces y después la primera producción , se obtiene

$$S \Rightarrow bS \Rightarrow bbS \Rightarrow \cdots \Rightarrow b^m.$$

Si aplicamos la segunda producción n veces y después la tercera producción m veces , se obtiene

$$S \Rightarrow aS \Rightarrow aaS \Rightarrow \cdots \Rightarrow a^nS \Rightarrow a^nbS \Rightarrow a^nbbS \Rightarrow \cdots \Rightarrow a^nb^m.$$

Si aplicamos la tercera producción m veces y después la segunda producción n veces , se obtiene

$$S \Rightarrow bS \Rightarrow bbS \Rightarrow \cdots \Rightarrow b^mS \Rightarrow b^maS \Rightarrow b^maaS \Rightarrow \cdots \Rightarrow b^ma^n.$$

Si se alternan la segunda y tercera producciones, se obtienen palabras del tipo

$$(ab)^n, \ (ba)^n.$$

Luego, el lenguaje generado por la gramática G es

$$L(G) = \{w \,|\, w = a^n,\ b^m,\ a^n b^m,\ b^m a^n,\ (ab)^n,\ (ba)^n,\ m, n \in \mathbb{N}\}.$$

Observe que siendo P finito puede generar lenguajes infinitos.

Ejemplo 3

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum_N = \{S\},\ \ \sum_T = \{0, 1\},\ \ P = \{S \to \lambda, S \to 0, S \to 1\}.$$

Solución

Es claro que el lenguaje generado por G es

$$L(G) = \{\lambda, 0, 1\}.$$

Ejemplo 4

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum_N = \{S\}, \ \sum_T = \{0, 1\}, \ \ P = \{S \to \lambda, S \to 0S1\}.$$

Solución

Es claro que el lenguaje generado por G es

$$L(G) = \{0^n 1^n \mid n \in \mathbb{N}\}.$$

Forma normal de BACKUS (FNB)

Es una notación que consiste en agrupar las producciones que tienen igual sus partes izquierdas, utilizando | para separar sus partes derechas. Por ejemplo, el conjunto P del ejemplo anterior puede ser escrito de la siguiente forma:

$$P = \{S \to \lambda \,|\, 0S1\}\,.$$

Ejemplo 5

Crear una gramática que genere el lenguaje $L(G) = \{1, 11, 111\} = \{1^n \,|\, n = 1, 2, 3\}$.

Solución

La gramática genera 3 palabras solamente y sólo tienen el símbolo 1. Por tanto, una solución posible es

$$G = \left(\sum_N, \sum_T, P, S\right),$$

donde $\sum_N = \{S\}, \quad \sum_T = \{1\}, \quad P = \{S \to 1 \,|\, 11 \,|\, 111\}.$

Ejemplo 6

Crear una gramática que genere el lenguaje $L(G) = \{1, 11, 111, 1111, \ldots\} = \{1^n \,|\, n > 0\}$.

Solución

La gramática genera palabras de uno o varios 1's. Por tanto, una solución posible es

$$G = \left(\sum_N, \sum_T, P, S\right),$$

donde $\sum_N = \{S, A\}, \quad \sum_T = \{1\}, \quad P = \{S \to A, A \to 1 \,|\, 1A\}$. o

$$G = \left(\sum_N, \sum_T, P, S\right),$$

donde $\sum_N = \{S\}, \quad \sum_T = \{1\}, \quad P = \{S \to 1 \,|\, 1S\}$.

Ejemplo 7

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$\sum_N = \{S, A\}$, $\sum_T = \{a\}$, $P = \{S \to \lambda \,|\, A, A \to AA \,|\, a\}$. Encuentre L(

Solución

$S \Rightarrow A \Rightarrow AA \Rightarrow AAA \Rightarrow aAA \Rightarrow aAAA \Rightarrow aaAA \Rightarrow aaAAA \Rightarrow \cdots \Rightarrow aaaAA \ldots$ Es claro que el lenguaje generado por G es

$$L(G) = \{\lambda, a, aa, aaa, \ldots\} = \{\lambda, a^n \,|\, n > 0\}.$$

Ejemplo 8

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$\sum_N = \{S, A\}$, $\sum_T = \{a, b\}$, $P = \{S \to \lambda \,|\, A, A \to aAb \,|\, ab\}$. Encuentre

Solución

$S \Rightarrow A \Rightarrow aAb \Rightarrow aaAbb \Rightarrow aaaAbbb \Rightarrow aaaaAbbbb \Rightarrow \cdots \Rightarrow$ $aaaaaa \ldots bbbbbb \ldots$ Es claro que el lenguaje generado por G es

$$L(G) = \{\lambda, ab, aabb, aaabbb, \ldots\} = \{\lambda, a^n b^n \,|\, n > 0\}.$$

1. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum\nolimits_N = \{S, A, B, C\}, \ \sum\nolimits_T = \{a, b, c\},$$

$$P = \left\{ \begin{array}{ccc} S \to \lambda, & S \to ABC, & A \to \lambda, \\ A \to aA, & B \to \lambda, & B \to bB, \\ C \to \lambda, & C \to cC & \end{array} \right\}.$$

2. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum_N = \{S, B, C\}, \ \sum_T = \{a, b, c\},$$

$$P = \left\{ \begin{array}{ccc} S \to aSBC, & S \to aBC, & CB \to BC, \\ aB \to ab, & bB \to bb, & bC \to bc, \\ cC \to cc & & \end{array} \right\}.$$

3. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum_N = \{S, A, B, C\}, \ \sum_T = \{a, b, c\},$$

$$P = \left\{ \begin{array}{ccc} S \to \lambda, & S \to aAbc, & Ab \to bB, \\ Bb \to bB, & Bc \to Ccc, & bC \to Cb, \\ aC \to aaAb, & A \to \lambda & \end{array} \right\}.$$

4. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum_N = \{S, A, B\}, \ \sum_T = \{a, b, c\},$$

$$P = \left\{ \begin{array}{ccc} S \to \lambda, & S \to aAbc, & Ab \to bA, \\ Ac \to Bbcc, & bB \to Bb, & aB \to aaA, \\ aB \to aa & & \end{array} \right\}.$$

5. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum_N = \{S\}, \ \sum_T = \{a, b\}, \ \ P = \{S \to ab, S \to aSb\}.$$

6. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum_N = \{S, A, B\}, \ \sum_T = \{a, b, c, d\}$$

y

$$P = \left\{ \begin{array}{ccc} S \to ASB, & A \to b, & aaA \to aaBB, \\ S \to d, & A \to aA, & B \to dcd \end{array} \right\}.$$

7. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum_N = \{S\}, \ \sum_T = \{0, 1\}, \ P = \{S \to 000S111, 0S1 \to 01\}.$$

8. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum_N = \{S\},\ \sum_T = \{0,1\},\ \ P = \{S \to 000S111, S \to 01\}.$$

9. Dadas las palabras siguientes de un lenguaje. Determinar las producciones que las generan:
$yxxyx,\ \ x,\ \ xyyx,\ \ (xyy)^n x,\ \ (yxxy)^n x$
10. Dado el lenguaje $L(G) = \{0^n 1^n \mid n \geq 1\}$. Determine las reglas de producción que lo generan.
11. Crear una gramática que genere el lenguaje $L(G) = \{\lambda, 1, 11, 111, 1111, \dots\} = \{1^n \mid n \geq 0\}$.

12. Crear una gramática que genere el lenguaje $L(G) = \{\lambda, 1, 11, 111\} = \{1^n \,|\, n = 0, 1, 2, 3\}$.
13. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde
$$\sum\nolimits_N = \{S, A\}, \;\; \sum\nolimits_T = \{a\}, \;\; P = \{S \to \lambda \,|\, A, A \to AaA \,|\, a\}.$$
14. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde
$$\sum\nolimits_N = \{S, A, B\}, \;\; \sum\nolimits_T = \{a, b\},$$
$$P = \{S \to aA, A \to b \,|\, aA \,|\, Bb, B \to Bb \,|\, b\}.$$

15. Encuentre el lenguaje generado si $G = (\sum_N, \sum_T, P, S)$ es una gramática, donde

$$\sum_N = \{S, A\}, \ \sum_T = \{a, b\}, \ \ P = \{S \to \lambda \,|\, A, A \to Ab \,|\, aA \,|\, a \,|\, b\}.$$

Jerarquía de Chomsky

Según Noam Chomsky las gramáticas se pueden clasificar en cuatro (4) tipos, atendiendo a restricciones que se les imponen a las producciones. Estas son las llamadas gramáticas tipo 0, tipo 1, tipo 2 y tipo 3. A continuación tenemos definición y características sobre cada una de ellas.

a. Gramáticas **Tipo 0 o sin restricciones (libres)**: Son gramáticas generales $G = (\sum_N, \sum_T, P, S)$ libres de restricciones. Las gramáticas que hemos tratado hasta el momento son de Tipo 0.

b. Gramáticas **Tipo 1 o dependientes del contexto (GDC)**: Son gramáticas $G = (\sum_N, \sum_T, P, S)$, donde cada producción $x \to y$ de P satisface la condición $|x| \leq |y|$. Por ejemplo, las gramáticas del ejemplo 1 y la del ejercicio 2 son de Tipo 1. En estas gramáticas, muchas veces se requiere que las producciones sean de la forma $\alpha_1 A \alpha_2 \to \alpha_1 \alpha \alpha_2$, donde $A \in \sum_N$ y $\alpha_1, \alpha_2, \alpha \in \sum^*, \;\; \alpha \neq \lambda$ y sólo se permite el reemplazo de A por α en el contexto de α_1 y α_2. Es posible que P posea la regla $S \to \lambda$.

Ejemplo

Dado el lenguaje $L(G) = \{a(bc)^n \,|\, n \geq 1\}$. Construir la gramática de tipo 1 que lo genera.

Solución

$$G = (\{S, B\}, \{a, b, c\}, P, S\},$$

donde

$$P = \{S \to aB, B \to bcB, B \to bc\}.$$

Ejemplo

Sea $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, B, C\}, \ \sum_T = \{a, b, c\}$$

y

$$P = \{S \to aSBC \,|\, abC, CB \to BC, bB \to bb, bC \to bc,$$
$$cB \to Bc, cC \to cc\}.$$

Verificar si la cadena $w = aabbcc$ es generada por G.

Solución

$$S \to aSBC \Rightarrow aabCBC \Rightarrow aabcBC \Rightarrow aabBcC \Rightarrow aabbcC \Rightarrow aabbcc.$$

Luego, la cadena es válida.

Derivemos la cadena $w = a^3b^3c^3$.

Solución

$$
\begin{aligned}
S \to aSBC &\Rightarrow aaSBCBC \Rightarrow aaabCBCBC \Rightarrow aaabBCCBC \\
&\Rightarrow aaabBCBCC \Rightarrow aaabBBCCC \Rightarrow aaabbBCCC \\
&\Rightarrow aaabbbCCC \Rightarrow aaabbbcCC \Rightarrow aaabbbccC \\
&\Rightarrow aaabbbccc = a^3b^3c^3.
\end{aligned}
$$

c. Gramáticas **Tipo 2 o independientes del contexto (GIC)**: Son gramáticas $G = (\sum_N, \sum_T, P, S)$, donde cada producción $x \to y$ de P satisface la condición de que x es una variable y y cualquier cadena diferente de λ.

En estas gramáticas, las producciones son de la forma $A \to \alpha$ y permiten que la variable A sea reemplazada por la cadena α independientemente del contexto en que aparece la A. Por ejemplo, la gramática $G = (\sum_N, \sum_T, P, S)$,donde

$$\sum_N = \{S, X, Y\}, \ \sum_T = \{a, b\}$$

y

$$P = \{\ S \to aY \,|\, bX, \quad X \to a \,|\, aS \,|\, bXX, \quad Y \to b \,|\, bS \,|\, aYY\ \},$$

es una gramática de Tipo 2.

Ejemplo

Dado el lenguaje $L(G) = \{0^n 1^n \,|\, n \geq 1\}$. Encontrar las reglas de producción que lo genera.

Solución

$$P = \{S \to 0S1, S \to 01\}.$$

Ejemplo

Dado el lenguaje $L(G) = \{a(bc)^n \mid n \geq 1\}$. Encontrar una gramática tipo 2 que lo genere.

Solución

$$G = (\{S, B\}, \{a, b, c\}, P, S\},$$

donde

$$P = \{S \to aB, B \to bcB, B \to bc\}.$$

La mayoría de los lenguajes de programación pueden ser representados por gramáticas del tipo 2.

Ejemplo

Consideremos la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum\nolimits_N = \{S, E\}, \;\; \sum\nolimits_T = \{+, *, (,), a, b, 0, 1\}$$

y

$$P = \left\{ \begin{array}{l} S \to E \,|\, S + S \,|\, S * S \,|\, (S), \\ E \to a \,|\, b \,|\, Ea \,|\, Eb \,|\, E0 \,|\, E1 \end{array} \right\}.$$

Derivar la cadena $a * (a + b00)$.

Solución

La derivación más a la izquierda es

$$\begin{aligned} S \;\Rightarrow\;& S*S \Rightarrow E*S \Rightarrow a*S \Rightarrow a*(S) \Rightarrow a*(S+S) \Rightarrow \\ & a*(E+S) \Rightarrow a*(a+S) \Rightarrow a*(a+E) \Rightarrow \\ & a*(a+E0) \Rightarrow a*(a+E00) \Rightarrow a*(a+b00) \end{aligned}$$

La derivación más a la derecha es

$$\begin{aligned} S \;\Rightarrow\;& S*S \Rightarrow S*(S) \Rightarrow S*(S+S) \Rightarrow S*(S+E) \Rightarrow \\ & S*(S+E0) \Rightarrow S*(S+E00) \Rightarrow S*(S+b00) \Rightarrow \\ & S*(E+b00) \Rightarrow S*(a+b00) \Rightarrow E*(a+b00) \Rightarrow \\ & a*(a+b00) \end{aligned}$$

d. Gramáticas **Tipo 3 o regulares (GR)**: Son gramáticas $G = (\sum_N, \sum_T, P, S)$, donde cada producción $x \to y$ de P es de la forma:

   1. Lineal por la derecha: $X \to aY$ o $X \to a$.
   2. Lineal por la izquierda: $X \to Ya$ o $X \to a$.

   Con X y Y variables y a un terminal. Se permiten también producciones de la forma $S \to \lambda$.

Ejemplo

La gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A\}, \ \sum_T = \{0, 1\}, P = \{S \to A1 \,|\, 1, A \to S0\}.$$

es lineal por la izquierda y genera el lenguaje

$$L(G) = \{1, 101, 10101, \dots\} = \{1(01)^n \mid n \geq 0\}$$

Ejemplo

La gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A\}, \ \sum_T = \{0, 1\}, P = \{S \to 1A \mid 1, A \to 0S\}.$$

es lineal por la derecha y genera el mismo lenguaje del ejemplo anterior

$$L(G) = \{1, 101, 10101, \dots\} = \{1(01)^n \mid n \geq 0\}$$

Ejemplo

La siguiente gramática es lineal por la derecha
$G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A, B\}, \ \sum_T = \{a, b\}$$

y

$$P = \left\{ \begin{array}{ccc} S \to aA, & S \to bB, & A \to aA, \\ A \to aS, & A \to bB, & B \to bB, \\ B \to b, & B \to a, & S \to a \end{array} \right\}.$$

Tipos de gramáticas

Cada gramática lineal por la izquierda tiene una gramática lineal por la derecha equivalente que genera el mismo lenguaje y viceversa.

Observemos que toda gramática regular es independiente del contexto; toda gramática independiente del contexto es dependiente del contexto y toda gramática dependiente del contexto es de Tipo 0. Los lenguajes generados por gramáticas Tipo 0 se les llama **Lenguajes Tipo 0**. De forma similar, los lenguajes generados por gramática dependiente del contexto, independiente del contexto o regular, se les llama respectivamente lenguajes dependiente del contexto, independiente del contexto o regular.

Contenido

Definición

Los Árboles de derivación son árboles utilizados para mostrar gráficamente la aplicación de las producciones que derivan cualquier cadena de un lenguaje a partir del símbolo de inicio o axioma de la gramática.

Los árboles de derivación satisfacen las propiedades siguientes:

a. El símbolo de inicio o axioma de la gramática es el vértice raíz del árbol y se coloca en la parte superior del árbol.
b. Todo vértice v está etiquetado con un símbolo de $\sum_N \cup \sum_T \cup \{\lambda\}$.
c. Los vértices internos están etiquetados con símbolos no terminales (símbolos de $\sum_N$).

Árboles de derivación

d. Si un vértice está etiquetado con A y sus m hijos están etiquetados con $X_1 X_2 \dots X_m$ (leídos de izquierda a derecha), entonces $A \to X_1 X_2 \dots X_m$ es una producción de la gramática.
e. Si un vértice está etiquetado con λ, entonces es el único hijo de un vértice.

Si todas las hojas son símbolos terminales o λ, entonces el árbol está **Completo** y su frontera es una palabra de $L(G)$.

El proceso de buscar un árbol de derivación para una cadena $v \in \sum_T^*$ se le llama **Análisis sintáctico** de v. Los árboles de derivación se les llama también **Árboles sintácticos o árboles de análisis sintácticos**.

Derivación a la izquierda significa que la sustitución empieza por el símbolo de más a la izquierda y **Derivación a la derecha**, por el símbolo de más a la derecha.

Ejemplo 1

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

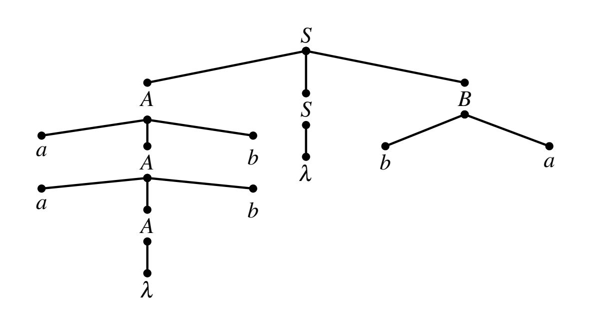
$$\sum_N = \{S, A, B\}, \ \sum_T = \{a, b\}$$

$$P = \{S \to \lambda \,|\, ASB, A \to aAb \,|\, \lambda, B \to bBa \,|\, ba\}.$$

Solución

La derivación
$S \Rightarrow ASB \Rightarrow aAbSB \Rightarrow aaAbbSB \Rightarrow aabbSB \Rightarrow aabbB \Rightarrow aabbba$ tiene como árbol de derivación a

Árboles de derivación



Ejemplo 2

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum_N = \{S\}, \;\; \sum_T = \{a, b, c\}$$

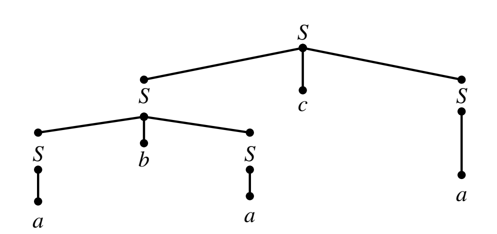
$$P = \{S \to SbS \,|\, ScS \,|\, a\}.$$

Solución

La derivación

$$S \Rightarrow ScS \Rightarrow SbScS \Rightarrow abScS \Rightarrow abacS \Rightarrow abaca$$

tiene como árbol de derivación a la izquierda a


S
S
c
S
S
b
S
a
a
a

Ejemplo 3

Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum_N = \{S\}, \ \sum_T = \{a, b, c\}$$

$$P = \{S \rightarrow SbS \,|\, ScS \,|\, a\}.$$

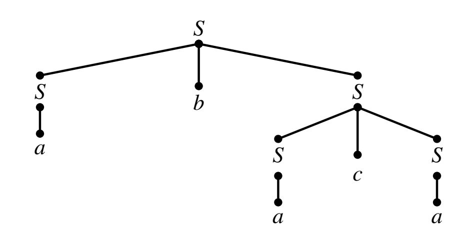
Solución

La derivación

$$S \Rightarrow SbS \Rightarrow abS \Rightarrow abScS \Rightarrow abacS \Rightarrow abaca$$

tiene como árbol de derivación a la izquierda a

Árboles de derivación



1. Determine el tipo de gramática según la jerarquía de Chomsky.
   a. $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum\nolimits_N = \{S, A, B\}, \ \sum\nolimits_T = \{a, b\},$$

$$P = \left\{ \begin{array}{lll} S \to aA, & A \to bB, & A \to aA, \\ A \to a, & B \to \lambda & \end{array} \right\}.$$

2. Compruebe que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum\nolimits_N = \{S, A\}, \ \sum\nolimits_T = \{a, b, c\}, \ P = \{S \to A, A \to aAa \,|\, bAb \,|\, c\}$$

genera el lenguaje $L(G) = \{wcw^{-1} \,|\, w \in \sum_T^*\}$.

3. Compruebe que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A, B, C\}, \ \sum_T = \{0, 1, 2, 3\}, \ \ P = \{S \to ABC \,|\, AC \,|\, BC$$

genera el lenguaje $L(G) = \{0^i 1^{i+k} 2^K 3^{n+1} \,|\, i, kn \geq 0\}$.

4. Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum_N = \{S\}, \ \sum_T = \{a, b\}, \ \ P = \{S \to ab \,|\, aSb\}.$$

Derive la cadena $aaabbb$ y encuentre el árbol de derivación.

5. Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum\nolimits_N = \{S, A, B\}, \ \sum\nolimits_T = \{a, b\},$$

$$P = \{S \to AB \,|\, AaB, A \to aA \,|\, a, B \to bBa \,|\, b\}.$$

Derive la cadena $abba$ de dos formas diferentes, pero con el mismo árbol de derivación (encuéntrelo).

6. Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum\nolimits_N = \{S, A, B, C\}, \ \sum\nolimits_T = \{a, b\},$$

$$P = \{S \to BAa, A \to bBC \,|\, a, B \to bB \,|\, b \,|\, \lambda, C \to aB \,|\, aa\}.$$

Derive la cadena $bbbaa$ y encuentre el árbol de derivación.

7. Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum_N = \{S, A, B\}, \ \sum_T = \{a, b\},$$

$$P = \{S \to aS \,|\, AaB, A \to aA \,|\, a, B \to bBbB \,|\, b\}.$$

Encuentre la derivación de la cadena $aaaabbb$ y encuentre el árbol de derivación.

8. Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum_N = \{S, A, B, C\}, \ \sum_T = \{a, b, c\},$$

$$P = \{S \to ABC, \mid BaC \mid aB, A \to Aa \mid a, B \to BAB \mid bab, C \to cC \mid \lambda\}$$

Halle las derivaciones de las cadenas $w_1 = abab, \ \ w_2 = babacc, \ \ w_3 = abababab c$ y encuentre los árboles de derivaciones.

9. Compruebe que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\}, \ \sum_T = \{a, b, c\}, \ \ P = \{S \to aSa \mid bSb \mid c\}$$

genera el lenguaje $L(G) = \{wcw^{-1} \mid w \in \sum_T^*\}$.

10. Compruebe que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum\nolimits_N = \{S\}, \ \ \sum\nolimits_T = \{a, b\}, \ \ P = \{S \to aSa \,|\, bSb \,|\, \lambda\}$$

genera el lenguaje $L(G) = \{ww^{-1} \,|\, w \in \sum_T^*\}$.

11. Compruebe que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum\nolimits_N = \{S\}, \ \ \sum\nolimits_T = \{a, b\}, \ \ P = \{S \to aSb \,|\, \lambda\}$$

genera el lenguaje $L(G) = \{a^n b^n \,|\, n \geq 0\}$.

12. Compruebe que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\},\ \sum_T = \{a, b\},\ \ P = \{S \to aSbb \,|\, \lambda\}$$

genera el lenguaje $L(G) = \{a^n b^{2n} \,|\, n \geq 0\}$.

13. Compruebe que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, B\},\ \sum_T = \{a, b, c\},\ \ P = \{S \to aSc \,|\, B, B \to bB \,|\, b\}$$

genera el lenguaje $L(G) = \{a^i b^k c^i \,|\, i \geq 0, k \geq 1\}$.

14. Sea $G = (\sum_N, \sum_T, P, S)$ una gramática, donde

$$\sum_N = \{S, A\}, \ \sum_T = \{0, 2, 4, 6, 8\},$$

$$P = \{S \to A \,|\, AS, A \to 0 \,|\, 2 \,|\, 4 \,|\, 6 \,|\, 8\}.$$

Derive la cadena 480 y encuentre el árbol de derivación.

15. Sea $P = \{S \to (A) \,|\, a, A \to A, S \,|\, S\}$. Halle
    a. $\sum_N$ y $\sum_T$
    b. ¿Cuál es símbolo inicial?.
    c. Encuentre los árboles de derivación de $(a, a), \ (a, (a, a))$ y $(a, ((a, a), (a, a)))$

16. Encuentre el lenguaje generado por las siguientes gramáticas

a. $G = (\sum_N, \sum_T, P, S)$ donde,

$$\sum_N = \{S, A, B\}, \ \sum_T = \{a\},$$

$$P = \{S \to \lambda \,|\, aA, A \to aB \,|\, a, B \to aA\}.$$

b. $G = (\sum_N, \sum_T, P, S)$ donde,

$$\sum_N = \{S, C, D\}, \ \sum_T = \{a\},$$

$$P = \{S \to \lambda \,|\, Ca, C \to Da \,|\, a, D \to Ca\}.$$

Definiciones

Una cadena o palabra $w \in L(G)$ es **Ambigua** si hay más de una derivación para w en la gramática.

La gramática $G = (\sum_N, \sum_T, P, S)$ es **Ambigua**, si existe $w \in L(G)$ con dos árboles de derivaciones diferentes o con al menos, dos derivaciones a la izquierda. Por ejemplo, la gramática del ejemplo 2 es ambigua.

No existe un algoritmo que permita saber con certeza si una gramática es o no ambigua.

Ejemplo 1

La gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\}, \ \sum_T = \{0, 1, +, *, (,)\}$$

$$P = \{S \to S + S \,|\, S * S \,|\, (S) \,|\, 0S \,|\, 1S \,|\, 0 \,|\, 1\}$$

es ambigua porque la cadena

$1 + 1 * 0$ tiene las siguientes derivaciones diferentes a la izquierda:

$$S \Rightarrow S + S \Rightarrow 1 + S \Rightarrow 1 + S * S \Rightarrow 1 + 1 * S \Rightarrow 1 + 1 * 0$$

$$S \Rightarrow S * S \Rightarrow S + S * S \Rightarrow 1 + S * S \Rightarrow 1 + 1 * S \Rightarrow 1 + 1 * 0.$$

Construya los árboles de derivación.

La ambigüedad puede eliminarse con el uso de paréntesis en las producciones como

$$S \to (S + S), \;\; S \to (S * S),$$

aunque esto genera el inconveniente de muchos paréntesis, lo que dificulta el análisis sintáctico.

Ejemplo 2

La gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A\}, \;\; \sum_T = \{a, b\}$$

$$P = \{S \to aSA \,|\, \lambda, A \to bA \,|\, \lambda\}$$

es ambigua porque la cadena

aab tiene dos derivaciones diferentes a la izquierda:

$$S \Rightarrow aSA \Rightarrow aaSAA \Rightarrow aaAA \Rightarrow aaA \Rightarrow aabA \Rightarrow aab$$

$$S \Rightarrow aSA \Rightarrow aaSAA \Rightarrow aaAA \Rightarrow aabAA \Rightarrow aabA \Rightarrow aab$$

Construya los árboles de derivación.

Ejemplo 3

La gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A\}, \ \sum_T = \{1\}$$

$$P = \{S \to 1A \,|\, 11, A \to 1\}$$

es ambigua porque la cadena

11 tiene dos derivaciones diferentes:

$$S \Rightarrow 11 \text{ y } S \Rightarrow 1A \Rightarrow 11$$

Ejemplo 4

La gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A\}, \ \sum_T = \{1\}$$

$$P = \{S \to 11\}$$

No es ambigua.

Tipos de ambigüedad

La ambigüedad la podemos clasificar en dos tipos:

a. Ambigüedad inherente
b. Ambigüedad transitoria

Ambigüedad inherente

Las ambigüedades inherentes tienen la característica de que no se pueden eliminar completamente, no importa la cantidad de transformaciones que se realicen sobre ellas. Estas gramáticas no pueden utilizarse para lenguajes de programación.

Un lenguaje $L(G)$ es **Inherentemente Ambiguo** si todas las gramáticas que generan el lenguaje son ambiguas. Por ejemplo, los lenguajes

$$L(G) = \{a^i b^j c^k \,|\, i = j \text{ o } j = k\}$$

y

$$L(G) = \{a^i b^i c^j d^j \,|\, i, j \geq 1\} \cup \{a^i b^j c^j d^i \,|\, i, j \geq 1\}$$

La gramática que genera el último de estos lenguajes es :

$$G = \left(\sum_N, \sum_T, P, S\right),$$

donde

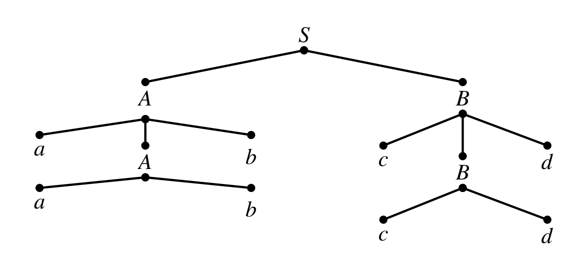
$$\sum_N = \{S, A, B, C, D\}, \ \sum_T = \{a, b, c, d\},$$

$$P = \left\{ \begin{array}{l} S \to AB \,|\, C, A \to aAb \,|\, ab, C \to aCd \,|\, aDd, \\ B \to cBd \,|\, cd, D \to bDc \,|\, bc \end{array} \right\}$$

La cadena $aabbccdd$ ($i = j = 2$) tiene las siguientes derivaciones a la izquierda :

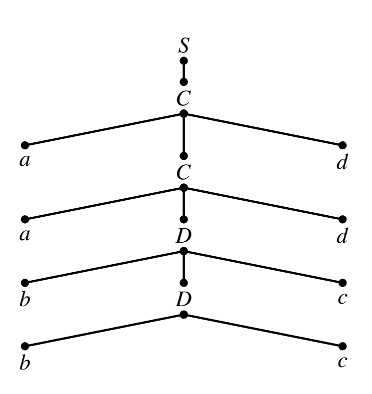
$$S \Rightarrow AB \Rightarrow aAbB \Rightarrow aabbB \Rightarrow aabbcBd \Rightarrow aabbccdd.$$

Su árbol de derivación es



$$S \Rightarrow C \Rightarrow aCd \Rightarrow aaDdd \Rightarrow aabDcdd \Rightarrow aabbccdd.$$

Su árbol de derivación es



En realidad, cualquier cadena donde $i = j$ tendrá dos derivaciones.

¿Por qué son ambiguas todas estas gramáticas?.

Si existe al menos una gramática G no ambigua para el lenguaje $L(G)$, entonces $L(G)$ es no ambiguo.

Ambigüedad transitoria

Estas ambigüedades tienen la característica de que pueden ser eliminadas aplicando una serie de transformaciones sobre la gramática original.

Definición

Una **Gramática está Limpia**, si carece de los elementos siguientes:

1. Producciones innecesarias : $A \to A$
2. Símbolos innaccesibles: $W \to A$ donde $W \in \sum_N, W \neq S$ (símbolo de inicio) no aparece en el lado derecho de alguna producción. W es accesible, si y sólo si, $S \Rightarrow xWy, x, y \in \sum^*$
3. Producciones supérfluas: Para no ser superflua debe satisfacer que $W \overset{+}{\Rightarrow} x,\ x \in \sum^*$.
4. Símbolos no generativos: Cada $A \in \sum_N$ debe generar al menos una cadena.

5. Producciones de redenominación: reglas de la forma $A \to B$ y $B \to X$ se sustituyen por la producción $A \to X$, donde $A, X \in \sum_N$.
6. Producciones no generativas: $A \to \lambda$. Si $L(G)$ no contiene a λ se pueden eliminar todas. En caso contrario, se pueden eliminar todas, excepto la producción $S \to \lambda$, donde cada $A \in \sum_N, \ \ A \neq S$ tal que $A \overset{*}{\Rightarrow} \lambda$ y por cada producción de la forma $B \to xAy$ se añadirá otra producción de la forma $B \to xy$, excepto si $x = y = \lambda$.
7. Ciclos : $S \to A, \ \ S \to a, \ \ A \to S$.
8. Producciones que producen caminos alternos: $S \to A, \ \ S \to B, \ \ A \to B$.

9. Producciones recursivas en que las variables no recursivas de la producción pueden derivar a la cadena vacía:

$$\{S \to ABS, S \to s, A \to a \,|\, \lambda, B \to b \,|\, \lambda\}$$

Definición

Una **Gramática bien formada** es aquella que está **Limpia** y no contiene producciones λ.

Ejemplo

Verificar si la gramática siguiente está bien formada. De lo contrario, convertirla a bien formada.

$G = (\sum_N, \sum_T, P, S)$, donde

$$\sum\nolimits_N = \{S, A, B, C\}, \ \sum\nolimits_T = \{0, 1\}$$

$$P = \{S \to AB \,|\, 0S1 \,|\, A \,|\, C, A \to 0AB \,|\, \lambda, B \to B1 \,|\, \lambda\}$$

Solución

1. Observamos que C es un símbolo no generativo, porque no aparece alguna regla que derive una palabra desde C. Por tanto, se puede sacar la producción $S \to C$ de P. Entonces la gramática se convierte en

$G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A, B, C\}, \ \sum_T = \{0, 1\}$$

$$P = \{S \to AB \,|\, 0S1 \,|\, A, A \to 0AB \,|\, \lambda, B \to B1 \,|\, \lambda\}$$

2. Eliminar las producciones de la forma $X \to \lambda$. Entonces la gramática se convierte en

   $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A, B, C\}, \ \sum_T = \{0, 1\}$$

$$P = \{S \to AB \,|\, 0S1 \,|\, A \,|\, B \,|\, \lambda, A \to 0AB \,|\, 0B \,|\, 0A \,|\, 0, B \to B1 \,|\, 1\}$$

3. Eliminar reglas de redenominación $S \to A \mid B$. De modo que la gramática se convierte en

   $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S, A, B, C\}, \ \sum_T = \{0, 1\}$$

$$P = \left\{ \begin{array}{l} S \to AB \mid 0S1 \mid 0AB \mid 0A \mid 0B \mid B1 \mid 0 \mid 1 \mid \lambda, \\ A \to 0AB \mid 0B \mid 0A \mid 0, \\ B \to B1 \mid 1 \end{array} \right\}$$

   Esta gramática es ya una gramática bien formada.

1. Muestre que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\},\ \ \sum_T = \{a, b\},\ \ P = \{S \to aSbS \mid bSaS \mid \lambda\}$$

   es ambigua.

2. Muestre que la gramática $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\},\ \ \sum_T = \{a, b, c\},\ \ P = \{S \to abS \mid abScS \mid \lambda\}$$

   es ambigua.

3. Considere la gramática ambigua $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\}, \ \sum_T = \{+, *, (,), 1, \ldots, 9\},$$

$$P = \{S \to S + S \,|\, S * S \,|\, (S), \,|\, 1 \,|\, \ldots \,|\, 9\}$$

Obtenga dos derivaciones para la cadena $S + S * S$ y encuentre sus árboles de derivación.

4. Considere la gramática ambigua $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\}, \ \sum_T = \{a\},$$

$$P = \{S \to aS \,|\, Sa \,|\, a\}$$

Obtenga dos derivaciones para la cadena aa y encuentre sus árboles de derivación.

5. Considere la gramática ambigua $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\}, \ \sum_T = \{+, *, (,), 1, \ldots, 9\},$$

$$P = \{S \to S + S \,|\, S * S \,|\, (S), \,|\, 1 \,|\, \ldots \,|\, 9\}$$

a. Encuentre dos árboles de derivación para la cadena $5 + 7 * 3$.
b. Obtenga una gramática no ambigua que derive la cadena $5 + 7 * 3$.

6. Considere la gramática ambigua $G = (\sum_N, \sum_T, P, S)$, donde

$$\sum_N = \{S\}, \ \sum_T = \{a\},$$

$$P = \{S \to aS \mid Sa \mid a\}$$

a. Encuentre dos árboles de derivación para la cadena aa.
b. Obtenga una gramática no ambigua que derive la cadena aa.

Contenido

Los lenguajes regulares se utilizan en la construcción de analizadores léxicos. EL conjunto de los lenguajes regulares sobre un alfabeto $\sum$ es el menor conjunto sobre $\sum$ que es cerrado respecto a las operaciones de concatenación, unión y cerradura de Kleene.

Antes de definir el conjunto de lenguajes regulares, enunciaré dos teoremas sobre los tamaños de $\sum^*$ y del conjnto de sublenguajes de este.

Teorema

El conjunto $\sum^*$ es infinito numerable (contable).

Teorema

El conjunto de sublenguajes de $\sum^*$ es infinito no numerable (no contable).

Definición

Dado un alfabeto $\sum$. Definimos el conjunto de lenguajes regulares recursivamente como:

a. $\emptyset = \{\}$ es un lenguaje regular.
b. $\{\lambda\}$ es un lenguaje regular.
c. $\{a\}$ es un lenguaje regular para todo $a \in \sum$.
d. Si L_1 y L_2 son lenguajes regulares, entonces $L_1 \cup L_2, \;\; L_1 L_2, \;\; L_1^*$ son lenguajes regulares.
e. Ningún otro lenguaje sobre $\sum$ es regular.

Ejemplo

Sea $\sum = \{a, b\}$ un alfabeto. Las expresiones siguientes representan lenguajes regulares.

1. $\emptyset$ y $\{\lambda\}$.
2. $\{a\}$ y $\{b\}$.
3. $\{a, b\}$ por la unión (item 2.).
4. $\{ab\}$ por con concatenación (item 2.).
5. $\{aa, ab, ba, bb\}$ por con concatenación (item 3.).
6. $\{a, ab, b\}$ por unión (items 3. y 4.).
7. $\{a^i \mid i \geq 0\}$ por concatenación (item 2.).
8. $\{b^j \mid j \geq 0\}$ por concatenación (item 2.).

9. $\{a^i b^j \mid i \geq 0, j \geq 0\}$ por concatenación (items 7. y 8.).
10. $\{(ab)^i \mid i \geq 0\}$ por concatenación (item 4.).
11. $\{bb\}$ por concatenación (item 2.).
12. $\{a, b\}^*$ por cerradura de Kleene (item 3.).
13. $\{a, b\}^* \{bb\} \{a, b\}^*$ por concatenación. Es el conjunto de cadenas que contiene la subcadena bb.
14. $\{a\} \{a, b\}^* \{b\} \{a, b\}^* \{a\}$ por concatenación. Es el conjunto de cadenas que empiezan y terminan en a y tiene al menos una b.

Ejemplo

El lenguaje sobre $\sum = \{a, b\}$ que consiste de todas las cadenas que contienen exactamente una a.

Solución

$$L = \{b\}^*\{a\}\{b\}^*$$

Ejemplo

El lenguaje sobre $\sum = \{a, b\}$ que consiste de todas las cadenas que comienzan con b.

Solución

$$L = \{b\}\{a, b\}^*$$

Ejemplo

El lenguaje sobre $\sum = \{a, b\}$ que consiste de todas las cadenas que contiene la subcadena ba.

Solución

$$L = \{a, b\}^*\{ba\}\{a, b\}^*$$

Ejemplo

Describir el lenguaje sobre $\sum = \{a, b\}$ que consiste de las cadenas que contienen la subcadena bb.

Solución

$$L = \{a, b\}^*\{bb\}\{a, b\}^*$$

Ejemplo

Describir el lenguaje sobre $\sum = \{a, b\}$ que consiste de las cadenas que empiezan con aa o terminan con bb.

Solución

$$L = \{aa\}\{a, b\}^* \cup \{a, b\}^*\{bb\}$$

Ejemplo

Describir el lenguaje sobre $\sum = \{a, b\}$ que consiste de las cadenas que contienen las subcadenas aa o bb o ambas subcadenas.

Solución

$$L = \{a, b\}^*\{aa\}\{a, b\}^* \cup \{a, b\}^*\{bb\}\{a, b\}^*$$

Definición

Una **Expresión regular** es una abreviatura para simplificar la descripción de un lenguaje regular. Por simplicidad se acostumbra a usar la siguiente notación:

1. El lenguaje $\{a\}$ se representa por a.
2. $\{a\} \cup \{b\}$ se representa por $a \cup b$.
3. $\{ab\}$ se representa por ab.
4. $\{a\}^*$ se representa por a^*.
5. $\{a\}^+$ se representa por a^+.

El orden de precedencia para las operaciones es: $*$ (primero), . (segundo) y $\cup$ (último). De este modo, expresiones como:

1. $\{bba\}^* \{a, b\}$ se escribe como $(bba)^* (a \cup b)$.
2. $\{b\}^* \{ba\}$ se escribe como $b^* ba$.
3. $(\{a\}^*\{b\}) \cup \{c\}$ se escribe como $a^*b \cup c$.
4. $\{a, ba\}^* (\{bb\}^* \cup \{aab, \lambda\})$ se escribe como $(a \cup ba)^* ((bb)^* \cup aab \cup \lambda)$.
5. $\{a\} \{a, b\}^* \{b\} \{a, b\}^* \{a\}$ se escribe como $a(a \cup b)^*(b)(a \cup b)^*a$.

La **definición recursiva de una expresión regular** sobre el alfabeto $\sum$ viene dada del modo siguiente:

1. $\emptyset$ y λ son expresiones regulares.
2. Para toda $a \in \sum$, a es una expresión regular.

3. Si s y t son expresiones regulares, entonces $s \cup t$, $s \cdot t$ y s^* son también expresiones regulares.
4. Ninguna otra secuencia de símbolos es una expresión regular.

Recordemos que tanto la unión como la concatenación son asociativas y además observe que

$$s^+ = ss^*.$$

Ejemplo

Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que empiezan con b y terminan con a.

Solución

$$b(a \cup b)^* a.$$

Ejemplo

Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que tienen exactamente dos (2) $a's$.

Solución

$$b^* a b^* a b^*.$$

Ejemplo

Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que tienen un número par de símbolos (palabras de longitud par).

Solución

$$(aa \cup ab \cup ba \cup bb)^*.$$

Ejemplo

Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que tienen un número impar de símbolos (palabras de longitud impar).

Solución

$$a(aa \cup ab \cup ba \cup bb)^* \cup b(aa \cup ab \cup ba \cup bb)^*.$$

Ejemplo

Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que tienen un número par de $a's$.

Solución

$$b^*(ab^*a)^*b^* \text{ ó } (ab^*a \cup b)^* \text{ ó } (b^*ab^*ab^*)^* \cup b^* \text{ ó } b^*(b^*ab^*ab^*)^*b^*.$$

Ejemplo

Sea $\sum = \{a, b, c\}$ un alfabeto. La expresión regular

$$(a \cup b^*)a^*(bc)^*$$

representa el lenguaje

$$(\{a\} \cup \{b\}^*)\{a\}^*\{bc\}^*.$$

Ejemplo

Sea $\sum = \{a, b\}$ un alfabeto. La expresión regular

$$(\lambda \cup a)^*(a \cup b)^*(ba)^*$$

representa el lenguaje

$$(\{\lambda\} \cup \{a\})^*\{a, b\}^*\{ba\}^*.$$

Ejemplo

Sea $\sum = \{a, b\}$ un alfabeto. Probar que el conjunto $\{bawab \,|\, w \in \{a, b\}^*\}$ es un lenguaje regular.

Prueba

Paso	Conjunto	Expresión	Justificación
$1.$	$\{a\}$	a	Base
$2.$	$\{b\}$	b	Base
$3.$	$\{a\}\{b\} = \{ab\}$	ab	Conc.
$4.$	$\{a\} \cup \{b\} = \{a, b\}$	$a \cup b$	Unión de 1. y 2.
$5.$	$\{b\}\{a\} = \{ba\}$	ba	Conc. de 2. y 1.
$6.$	$\{a, b\}^*$	$(a \cup b)^*$	Cerr. Kleene de 4.
$7.$	$\{ba\}\{a, b\}^*$	$ba(a \cup b)^*$	Conc. de 5. y 6.
$8.$	$\{ba\}\{a, b\}^*\{ab\}$	$ba(a \cup b)^*ab$	Conc. de 7. y 3.

Ejemplo

Escriba una expresión regular para el lenguaje sobre el alfabeto $\sum = \{a, b\}$ que consiste de las cadenas en las que no hay dos símbolos iguales contiguos. Es decir, las $a's$ y las $b's$ se alternan.

Solución

$(ab)^* \cup (ba)^* \cup a(ba)^* \cup b(ab)^*$ o
$(\lambda \cup b)(ab)^*(\lambda \cup a)$ o
$(\lambda \cup a)(ba)^*(\lambda \cup b)$

Ejemplo

Escriba una expresión regular para el lenguaje sobre el alfabeto $\sum = \{a, b\}$ que consiste de las cadenas que contienen dos (2) o más $b's$.

Solución

$$\{a\}^*\{b\}\{a\}^*\{b\}\{a,b\}^* \cup \{a,b\}^*\{b\}\{a\}^*\{b\}\{a\}^* \cup \{a,b\}^*\{b\}\{a,b\}^*\{b\}\{a,b\}^*$$

Para indicar que L es el lenguaje representado por la expresión regular r se escribe $L(r)$

Equivalencias

1. Una cadena pertenece al lenguaje representado por una expresión regular, si y sólo si, sigue el patrón definido por la expresión regular.

2. Las expresiones regulares que representan lenguajes deben cumplir con las siguientes condiciones:
    a. **Correcta:** Todas las cadenas representadas por la expresión regular deben pertenecer al lenguaje.
    b. **Completa:** Toda palabra del lenguaje debe ser representada por la expresión regular.
3. La concatenación indica orden de los símbolos, la cerradura de Kleene permite repetición y la unión indica selección.
4. Si dos expresiones regulares r y s representan el mismo lenguaje, es decir, si $L(r) = L(s)$, se dice que r y s son **Equivalentes**.

Si w es una cadena generada por la expresión regular r, se escribe que $w \in L(r)$. Cuando r y s son equivalentes se puede escribir $r = s$. Si $L(r) \subseteq L(s)$ se puede escribir $r \subseteq s$.

Nota:

La representación de lenguajes regulares mediante expresiones regulares no es única. Es decir, es posible que existan expresiones regulares distintas para el mismo lenguaje.

Ejemplo

Las expresiones regulares

$$b(a \cup b)^* \text{ y } b(b \cup a)^*$$

representan el mismo lenguaje.

Ejemplo

Las expresiones

$$(a \cup b)^* \text{ y } (a^* b^*)^*$$

representan el mismo lenguaje.

Ejemplo

$$(a^* b)^* \text{ y } \lambda \cup (a \cup b)^* b$$

representan el mismo lenguaje. Este es el lenguaje que tienen 0 ó más $a's$ y $b's$. Entonces se puede escribir

$$(a^*b)^* = \lambda \cup (a \cup b)^*b.$$

Identidades

Sean r, s y t expresiones regulares sobre el alfabeto $\sum$. Entonces

1. $r\emptyset = \emptyset r = \emptyset$.
2. $r\lambda = \lambda r = r$.
3. $\emptyset^* = \lambda$.
4. $\lambda^* = \lambda$.
5. $r \cup s = s \cup r$.

6. $r \cup \emptyset = \emptyset \cup r = r$.
7. $r \cup r = r$.
8. $(r \cup s) \cup t = r \cup (s \cup t)$.
9. $(rs)t = r(st)$.
10. $r(s \cup t) = rs \cup rt$ y $(r \cup s)t = rt \cup st$.
11. $r^* = r^{**} = r^*r^* = (\lambda \cup r)^* = r^*(r \cup \lambda) = (r \cup \lambda)r^* = \lambda \cup rr^*$.
12. $(r \cup s)^* = (r^* \cup s^*)^* = (r^*s^*)^* = (r^*s)^*r^* = r^*(sr^*)^*$.
13. $r(sr)^* = (rs)^*r$.
14. $(r^*s)^* = \lambda \cup (r \cup s)^*s$.
15. $(rs^*)^* = \lambda \cup r(r \cup s)^*$.
16. $s(r \cup \lambda)^*(r \cup \lambda) \cup s = sr^*$.

17. $rr^* = r^*r$.

Ejemplo

Simplicar la expresión regular $b^*(ab^*)^* \cup b^*(ab^*)^*a$ sobre el alfabeto $\sum = \{a, b\}$.

Solución

$$\begin{aligned} b^*(ab^*)^* \cup b^*(ab^*)^*a &= b^*(ab^*)^*(\lambda \cup a) & \text{(ident 10)} \\ &= (b \cup a)^*(\lambda \cup a) & \text{(ident 12)} \end{aligned}$$

Ejemplo

Simplicar la expresión regular $a \cup a(b \cup aa)(b^*aa)^*b^* \cup a(aa \cup b)^*$ sobre el alfabeto $\sum = \{a, b\}$.

Solución

$a \cup a(b \cup aa)(b^*aa)^*b^* \cup a(aa \cup b)^* =$

$$
\begin{aligned}
&= a \cup a(b \cup aa)(b \cup aa)^* \cup a(aa \cup b)^* && \text{(ident 12)}\\
&= a(\lambda \cup (b \cup aa)(b \cup aa)^*) \cup a(aa \cup b)^* && \text{(ident 10)}\\
&= a(b \cup aa)^* \cup a(aa \cup b)^* && \text{(ident 11)}\\
&= a(aa \cup b)^* \cup a(aa \cup b)^* && \text{(ident 5)}\\
&= a(aa \cup b)^* && \text{(ident 7)}
\end{aligned}
$$

Ejemplo

Simplicar la expresión regular $1^*O1^*O(O1^*O1^*O \cup 1)^*O1^* \cup 1^*$ sobre el alfabeto $\sum = \{0, 1\}$ de modo que sólo aparezca una operación $\cup$.

Solución

$1^*O1^*O(O1^*O1^*O \cup 1)^*O1^* \cup 1^* =$

$$
\begin{aligned}
&= 1^*O1^*O(1 \cup O1^*O1^*O)^*O1^* \cup 1^* && \text{(ident 5)}\\
&= 1^*O1^*O(1^* \cdot O1^*O1^*O)^*1^* \cdot O1^* \cup 1^* && \text{(ident 12)}\\
&= (1^*O1^*O \cdot 1^*O)^*1^*O1^*O1^*O1^* \cup 1^* && \text{(ident 13)}\\
&= ((1^*O1^*O1^*O)^*1^*O1^*O1^*O \cup \lambda)1^* && \text{(ident 10)}\\
&= (1^* \cdot O1^*O1^*O)^*1^* && \text{(ident 11)}\\
&= (1 \cup O1^*O1^*O)^* && \text{(ident 12)}
\end{aligned}
$$

1. Considere los lenguajes $L_1 = \{bb\}$ y $L_2 = \{\lambda, bb, bbbb\}$. Qué características tienen las cadenas de L_1^* y L_2^*?.
2. Encuentre la expresión regular sobre $\sum = \{a, b\}$ que representa el lenguaje de todas las cadenas que tengan a la subcadena aa o a la subcadena bb o a ambas subcadenas.
3. Encuentre la expresión regular sobre $\sum = \{a, b\}$ que representa el lenguaje de todas las cadenas que contengan exactamente dos (2) $b's$.
4. Encuentre la expresión regular sobre $\sum = \{a, b\}$ que representa el lenguaje de todas las cadenas que contengan un número par de $b's$.

5. Encuentre la expresión regular sobre $\sum = \{a, b\}$ que representa el lenguaje de todas las cadenas en las que aparezca una a inmediatamente antes de toda b.
6. Encuentre la expresión regular sobre $\sum = \{a, b\}$ que representa el lenguaje de todas las cadenas en las que aparezca exactamente una vez dos (2) $b's$ contiguas.
7. ¿Qué características tienen las cadenas sobre $\sum = \{a, b\}$ representada por $\{aa, bb, ab, ba\}$?.
8. ¿Qué características tienen las cadenas del lenguaje sobre $\sum = \{a, b\}$ representado por $\{a, b\}^* - \{aa, bb, ab, ba\}^*$?. ¿Es un lenguaje regular?.

9. ¿Qué características tienen las cadenas del lenguaje sobre $\sum = \{a, b\}$ representado por $c^*(b \cup ac^*)^*$?.
10. Encuentre una expresión regular que represente las cadenas sobre $\sum = \{a, b\}$ de longitud igual a 6.
11. Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que tienen la subcadena ab un número par de veces.
12. Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que tienen un número impar de $a's$.

13. Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que tienen un número par de $a's$ o un número impar de $b's$.
14. Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b, c\}$ de todas las cadenas que tienen un número par de símbolos.
15. Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b, c\}$ de todas las cadenas que tienen un número impar de símbolos.
16. Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b, c\}$ de todas las cadenas que comienzan con c y terminan con b.

17. Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b, c\}$ de todas las cadenas que no contienen la subcadena cc.

18.(*) Encuentre una expresión regular que represente el lenguaje definido sobre $\sum = \{a, b\}$ de todas las cadenas que tienen un número par de $a's$ y un número impar de $b's$.

19. Simplifique la expresión regular $c^*c \cup c^*$.

20. Simplifique la expresión regular $c \cup c^*$.

Nota:

No todos los lenguajes sobre un alfabeto $\sum$ son regulares.

Ejemplo

El lenguaje

$$L = \{a^n b^n \,|\, n \geq 0\}$$

sobre $\sum = \{a, b\}$ no puede ser representado por una expresión regular. Por tanto, no es un lenguaje regular.

Contenido

Definición

Un **Autómata finito o máquina de estado finito** M es un modelo matemático de un sistema que recibe de entrada una cadena formada por símbolos de un alfabeto y de dependiendo de los estados que asuma en cada momento el autómata determina si la cadena pertenece o no al lenguaje que éste reconoce. Los autómatas finitos son utilizados para reconocer lenguajes regulares. El objetivo de los autómatas finitos es saber si una cadena dada pertenece o no al lenguaje regular reconocido por el autómata.

Si la cadena es reconocida como válida por el autómata se dice que es **Aceptada (legal)**. En caso contrario, se dice que es **Rechazada (ilegal)**.

Formalmente, un autómata finito (AF), M, es una 5-$tupla$, tal que

$$M = \left(Q, \sum, q_0, \delta, F\right),$$

donde

1. Q es un conjunto finito no vacío de estados.
2. $\sum$ es un alfabeto de entrada.
3. $q_0 \in Q$ es un estado inicial.
4. $F \subseteq Q$ es un conjunto de estados finales o de aceptación.
5. $\delta : Q \times \sum \to Q$ es una función asociada a M, llamada **Función de transición.**

Tipos de autómatas finitos

Los autómatas finitos se clasifican en:

1. **Deterministas (AFD):** son aquellos donde cada par $(q, a),\ q \in Q, a \in \sum$, de entrada a la función de transición δ, produce un solo estado. En otras palabras, el autómata sólo puede estar en un estado en un momento determinado.
2. **No deterministas (AFND):** son aquellos donde cada par definido $(q, a),\ q \in Q, a \in \sum$, de entrada a la función de transición δ, puede producir varios estados. Además se permiten las transiciones-λ. Es decir, el autómata puede estar en varios estados al mismo tiempo.

Representación

Los autómatas finitos se pueden representar por medio de:

1. **Tablas de transición o matrices de estados:** son aquellas formadas por filas y columnas, donde las filas están encabezadas por los estados y las columnas por los símbolos del alfabeto. La intersección de una fila q (estado) con una columna a (símbolo de entrada) corresponde al estado $\delta(q, a)$.
2. **Diagramas de transición:** son grafos dirigidos con las características siguientes:
   a. Los vértices son etiquetados con los elementos de Q (estados).
   b. Las aristas **(transiciones)** son etiquetadas con los símbolos de $\sum$ (alfabeto).

c. q_0 (estado inicial) se marca con una $\rightarrow$.
d. Los estados finales se marcan con doble círculo o con $*$.

Ejemplo

Consideremos el autómata finito determinista

$$M = (Q, \sum, q_0, \delta, F),$$

donde $Q = \{q_0, q_1, q_2\}$, $\sum = \{a, b\}$, $F = \{q_0\}$ y δ, definida por medio de la tabla de transición:

δ	a	b
$\rightarrow *q_0$	q_1	q_2
q_1	q_2	q_0
q_2	q_2	q_2

Esta tabla significa que:

$$\delta(q_0, a) = q_1,\ \delta(q_0, b) = q_2,\ \delta(q_1, a) = q_2,$$

$$\delta(q_1, b) = q_0,\ \delta(q_2, a) = q_2,\ \delta(q_2, b) = q_2.$$

Es decir, la función de transición produce el estado al que se desplaza el autómata desde un par estado-símbolo de entrada.

Ejemplo

Verificar si la cadena $ababab$ es aceptada por el autómata anterior.

Solución

Para que la cadena sea aceptada, el estado que produce la última b debe pertenecer a F. En este caso, debe ser q_0. Veamos

$$\delta(q_0, a) = q_1,\ \delta(q_1, b) = q_0,\ \delta(q_0, a) = q_1,$$
$$\delta(q_1, b) = q_0,\ \delta(q_0, a) = q_1,\ \delta(q_1, b) = q_0.$$

Como la última b produjo el estado q_0 (estado final), la cadena es aceptada. En realidad, este autómata acepta la expresión regular $(ab)^*$. Es claro que este autómata es determinista.

Ejemplo

Verificar si la cadena $abbb$ es reconocida o rechazada por el autómata anterior.

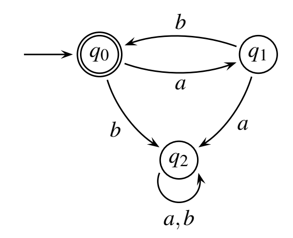
Solución

$$\delta(q_0, a) = q_1,\ \delta(q_1, b) = q_0,\ \delta(q_0, b) = q_2,\ \delta(q_2, b) = q_2.$$

Como $q_2 \notin F$, la cadena es rechazada.

Ejemplo

El diagrama de transición que representa el autómata del ejemplo anterior es:



Ejemplo

Dado el autómata finito determinista $M = (Q, \sum, q_0, \delta, F)$, donde

$$Q = \{q_0, q_1, q_2\}, \ \ \sum = \{a, b\}, \ \ F = \{q_1\}$$

y δ definida como

$$\delta(q_0, a) = q_1, \ \ \delta(q_0, b) = q_2, \ \ \delta(q_1, a) = q_1,$$

$$\delta(q_1, b) = q_2, \ \ \delta(q_2, a) = q_2, \ \ \delta(q_2, b) = q_2.$$

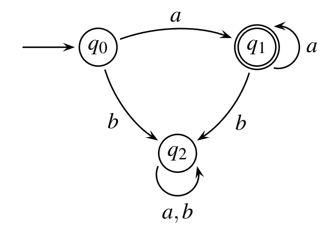
Encontrar su tabla de transición y diagrama de transición.

Solución

Tabla de transición:

δ	a	b
$\rightarrow q_0$	q_1	q_2
$*q_1$	q_1	q_2
q_2	q_2	q_2

Diagrama de transición:



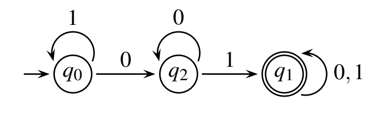
Ejemplo

Consideremos el autómata finito determinista $M = (Q, \sum, q_0, \delta, F)$, donde

$$Q = \{q_0, q_1, q_2\}, \ \sum = \{0, 1\}, \ F = \{q_1\}.$$

La función de transición δ se define por medio de la tabla o diagrama de transición siguientes:

δ	0	1
$\rightarrow q_0$	q_2	q_0
$*q_1$	q_1	q_1
q_2	q_2	q_1



Observación:

En los autómatas finitos deterministas no existen transisicones λ. Además, para toda $q \in Q$ y para todo $a \in \sum$, se tiene que $\delta(q, a)$ es única.

Note que para cada $q \in Q$ y cada $a \in \sum$, la función $\delta(q, a)$ produce otro estado de Q, que se combina con el próximo símbolo de la cadena de entrada para generar otro estado de Q y así sucesivamente. Es decir, la aplicación de la transición δ es recursiva sobre los símbolos de la cadena de entrada.

Por ejemplo, supongamos que q_0 es el estado inicial de un autómata finito M. Si la cadena de entrada es abc, la aplicación recursiva de δ sería

$$\delta(\delta(\delta(q_0, a), b), c).$$

Definición (función de transición asociada a cadena)

Si $M = (Q, \sum, q_0, \delta, F)$ es un AFD, definimos la función de transición asociada a cadena como

$$\delta' : Q \times \sum^* \to Q,$$

donde

a. $\delta'(q, \lambda) = q$

b. $\delta'(q, a) = \delta(q, a)$

c. $\delta'(q, aw) = \delta'(\delta(q, a), w)$

con $w \in \sum^*$, $a \in \sum$, $q \in Q$.

Definición

Decimos que los AFD M_1 y M_2 son **Equivalentes** si $L(M_1) = L(M_2)$. Es decir, si reconocen el mismo lenguaje.

Recordemos que

$$L(M) = \{w \in \sum^* \Big| \delta'(q_0, w) \in F\}.$$

De manera formal, una cadena $w \in \sum^*$ es **Aceptada** por el autómata $M = (Q, \sum, q_0, \delta, F)$, si y sólo si, $\delta'(q_0, w) \in F$. En caso contrario, la cadena w es **Rechazada**

Ejemplo

Los autómatas sobre el alfabeto $\{1\}$, representados por los diagramas de transición siguientes son equivalentes.



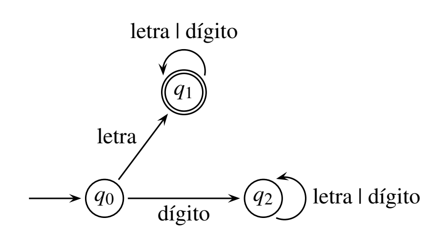
Estos autómatas aceptan el lenguaje 1^+.

Ejemplo

Construir tabla y diagrama de transición para un AFD que reconozca variables que empiecen con letra y siga con letra y/o dígito.

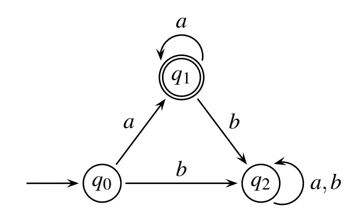
Solución

δ	letra	dígito
$\rightarrow q_0$	q_1	q_2
$*q_1$	q_1	q_1
q_2	q_2	q_2



Ejemplo

Considere el autómata finito dado por el siguiente diagrama de transición. Determine si el autómata reconoce o rechaza la cadena $aabbaba$.

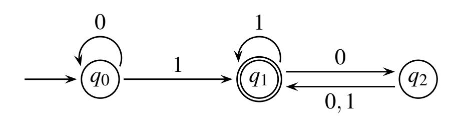


Solución

Si el autómata parte del estado q_0 y recibe el símbolo a, pasa al estado q_1. Si recibe el símbolo a de nuevo, se mantiene en el estado q_1. Si ahora recibe el símbolo b, pasa al estado q_2. Si recibe el símbolo b de nuevo, se queda en el estado q_2. Si ahora recibe el símbolo a, se queda en el estado q_2. Si recibe el símbolo b, se queda en el estado q_2. Si recibe el símbolo a, se mantiene el estado q_2. Como el último símbolo dejó el autómata en el estado q_2 y q_2 no es estado final, se dice que la cadena no es reconocida por el autómata y por tanto, es **rechazada**.

Ejemplo

Consideremos el AFD definido por el diagrama de transición



¿Cuál es la secuencia de estados que se genera con la entrada 011?

Solución

La secuencia es (q_0, q_0, q_1, q_1).

Minimización de AFD por conjunto cociente

Este proceso consiste en encontrar un AFD con la menor cantidad de estados posibles y equivalente a un AFD dado.

Definición

Sea $M = (Q, \sum, q_0, \delta, F)$ un AFD. Entonces

a. q_0 es **Alcanzable o accesible**

b. Si $q \in Q$ es alcanzable o accesible, entonces $\forall a \in \sum$, se tiene que $\delta(q, a)$ es **Alcanzable**.

Es decir, un estado $p \in Q$ es **Alcanzable o accesible** desde un estado $q \in Q$, si $\delta(q, a) = p,\ a \in \sum$. En caso contrario, se dice que p es **Inalcanzable o inaccesible** desde q.

Definición

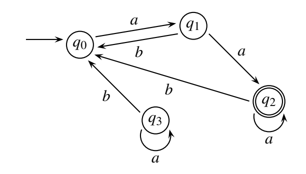
Se dice que un estado $q \in Q$ es **Accesible o alcanzable** desde el estado inicial (q_0), si $\exists \alpha \in \sum^* \ni \delta'(q_0, \alpha) = q$. En caso contrario, se dice que q es **Inaccesible o inalcanzable** desde el estado inicial.

Definición

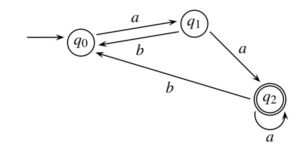
Un AFD es **Conexo** si todos sus estados son accesibles desde el estado inicial. En caso contrario, se dice que es **No conexo**.

Ejemplo

En el siguiente autómata el estado q_3 es inaccesible. Por tanto, el AFD es no conexo.



si se elimina el estado inaccesible q_3 y todas sus transiciones, se obtiene el AFD conexo siguiente, que es equivalente al anterior.



Definición

Sea $M = (Q, \sum, q_0, \delta, F)$ un AFD. Decimos que los estados $p, q \in Q$ son **Equivalentes** , si

$$\forall \alpha \in \sum^{*} : \delta(p, \alpha) \in F \Leftrightarrow \delta(q, \alpha) \in F.$$

Se escribe $p\, E\, q$. Observe que esta es la definición de una relación de equivalencia.

Es decir, si para toda secuencia de entrada, ambos producen la misma salida, sin importar cuál sea el estado inicial. En otras palabras, si al unirse en un solo estado reconocen el mismo lenguaje regular, tal como si estuvieran separados. Esto incluye la unión de sus transiciones tanto de entrada como de salida.

El conjunto de estados del AFD mínimo corresponde al conjunto cociente (Q/E) de esta relación de equivalencia de estados.

Definición

Dados $p, q \in Q$ y $k \in \mathbb{N}$. Se dice que p y q son **Equivalentes en longitud** k **o** k**-equivalentes**, si

$$\forall \alpha \in \sum^{*}, \ |\alpha| \leq k : \delta(p, \alpha) \in F \Leftrightarrow \delta(q, \alpha) \in F.$$

Se escribe $p\,E_k\,q$.

Para cada k, E_k es una relación de equivalencia. Es claro que

$$p\,E\,q \Leftrightarrow p\,E_k\,q,\ \forall k \geq 0.$$

Definición

Sea $M = (Q, \sum, q_0, \delta, F)$ un AFD. Decimos que los estados $p, q \in Q$ son **No equivalentes** si existe una palabra, $\alpha \in \sum^*$, para la cual, ambos producen salidas diferentes, sin importar cuál sea el estado inicial.

Definición

Sea $M = (Q, \sum, q_0, \delta, F)$ un AFD. Decimos que los estados $p, q \in Q$ son **Compatibles** si ambos, o pertenecen a F (conjunto de estados finales) o pertenecen a $Q - F$ (conjunto de estados no finales). En caso contrario, se dice que son **Incompatibles**.

Nota: Un estado final y un estado no final nunca serán equivalentes.

Decimos que un AFD está **Minimizado** si todos sus estados son distinguibles y alcanzables.

Algoritmo para determinar el conjunto cociente

a. Eliminar todos los estados inaccesibles, junto a todas sus transiciones.

   Sabemos que $\delta(q, \lambda) = q$. Ahora aplicamos recursividad sobre k.

b. Para $k = 0$.
   Los estados q_1 y q_2 son equivalentes de orden 0, solamente si, $q_1, q_2 \in F$ (estados finales) o sólo si, $q_1, q_2 \in F^c$ (estados no finales). De este modo, el conjunto cociente de la relación de equivalencia E_0 será

$$Q/E_0 = \{C_{01} = F, C_{02} = F^c\}.$$

c. Suponga que se ha calculado el conjunto cociente para la relación de equivalencia de estados de orden k:

$$Q/E_k = \{C_{k1}, C_{k2}, C_{k3}, \ldots, C_{km}\}.$$

d. Encontrar Q/E_{k+1}.

Para cada $C_{ki} \in Q/E_k,\ i \in \{1, 2, 3, \ldots, m\}$ se presenta uno y sólo uno de los casos siguientes:

1. Para todo $a \in \sum$, existe $j \in \{1, 2, 3, \ldots, m\}$ tal que $\delta(C_{ki}, a) \subseteq C_{kj}$. En este caso se incluye C_{ki} en Q/E_{k+1}.

2. Existe $a \in \sum$, tal que para cada $j \in \{1, 2, 3, \ldots, m\}, \ \delta(C_{ki}, a) \not\subset C_{kj}$. En este caso se hace $C_{ki} = C_{ki1} \cup C_{ki2}$ (una partición de C_{ki}), de modo que para cada uno de los subconjuntos creados existan j y m, tales que $\delta(C_{ki1}, a) \subseteq C_{kj}$ y $\delta(C_{ki2}, a) \subseteq C_{km}$. En este caso se incluye C_{ki1} y C_{ki2} en Q/E_{k+1} y se elimina C_{ki}.

e. Si $Q/E_k = Q/E_{k+1}$ se termina el proceso y $Q/E = Q/E_k$. En caso contrario, se repite el procedimiento desde el paso d.

Sea $M = (Q, \sum, q_0, \delta, F)$ un AFD. Existe un AFD único equivalente mínimo (autómata del conjunto cociente)

$$M_m = (Q_m, \sum, q_{0m}, \delta_m, F_m),$$

donde

a. $Q_m = Q/E$.

b. $\forall a \in \sum, \quad \delta_m(C_i, a) = C_j, \;$ si $\; \exists q_1 \in C_i, \; q_2 \in C_j \ni \delta(q_1, a) = q_2$.

c. $q_{0m} = C_0$ si $q_0 \in C_0$ y $C_0 \in Q_m$.

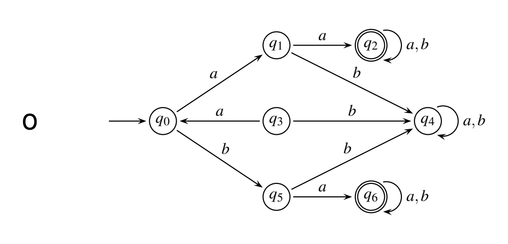
d. $F_m = \{C_i \,|\, \exists q \in C_i, \; q \in F\}$

Ejemplo

Minimizar el AFD $M = (\{q_0, q_1, q_3, q_4, q_5\}, \{a, b\}, q_0, \delta, \{q_2, q_6\})$, definido por

δ	a	b
$\rightarrow q_0$	q_1	q_5
q_1	q_2	q_4
$*q_2$	q_2	q_2
q_3	q_0	q_4
q_4	q_4	q_4
q_5	q_6	q_4
$*q_6$	q_6	q_6

o



Solución

Empezamos con $Q/E_0 = \{C_{01} = \{q_2, q_6\}, C_{02} = \{q_0, q_1, q_4, q_5\}\}$
$\delta(\{q_2, q_6\}, a) = \{q_2, q_6\} \subseteq C_{01}$.
$\delta(\{q_2, q_6\}, b) = \{q_2, q_6\} \subseteq C_{01}$.
$\delta(\{q_0, q_1, q_4, q_5\}, a) = \{q_1, q_2, q_4, q_6\} \not\subseteq C_{0j},\ \forall j \in \{1, 2\}$.
$C_{02} = C_{021} \cup C_{022}, \quad C_{021} = \{q_0, q_4\}, \quad C_{022} = \{q_1, q_5\}$

$$Q/E_1 = \{C_{11} = \{q_2, q_6\}, C_{12} = \{q_0, q_4\}, C_{13} = \{q_1, q_5\}\}$$

Como $Q/E_0 \neq Q/E_1$, el proceso continúa.

$\delta(C_{11}, a) = \{q_2, q_6\} \subseteq C_{11}$
$\delta(C_{11}, b) = \{q_2, q_6\} \subseteq C_{11}$

$\delta(C_{12}, a) = \{q_1, q_4\} \not\subset C_{1j}, \quad \forall j \in \{1, 2, 3\}$
$C_{12} = C_{121} \cup C_{122}, \quad C_{121} = \{q_0\}, \quad C_{122} = \{q_4\}$
$\delta(C_{13}, a) = \{q_2, q_6\} \subseteq C_{11}$
$\delta(C_{13}, b) = \{q_4\} \subseteq C_{12}$

$$Q/E_2 = \{C_{21} = \{q_2, q_6\}, C_{22} = \{q_0\}, C_{23} = \{q_4\}, C_{24} = \{q_1, q_5\}\}$$

Como $Q/E_1 \neq Q/E_2$, el proceso sigue.

$\delta(C_{21}, a) = \{q_2, q_6\} \subseteq C_{21}$
$\delta(C_{21}, b) = \{q_2, q_6\} \subseteq C_{21}$

Las clases que tienen un solo elemento no es necesario comprobarla.

$\delta(C_{24}, a) = \{q_2, q_6\} \subseteq C_{21}$

Minimización de AFD por conjunto cociente

$\delta(C_{24}, b) = \{q_4\} \subseteq C_{23}$

$$Q/E_3 = \{C_{31} = \{q_2, q_6\}, C_{32} = \{q_0\}, C_{33} = \{q_4\}, C_{34} = \{q_1, q_5\}\}$$

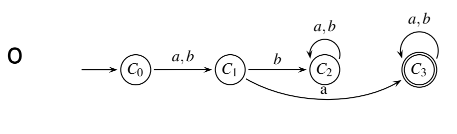
Como $Q/E_2 = Q/E_3$, se tiene que $Q/E = Q/E_2$. Luego,

$$Q/E = \{C_3 = \{q_2, q_6\}, C_0 = \{q_0\}, C_2 = \{q_4\}, C_1 = \{q_1, q_5\}\}.$$

y el AFD mínimo es

δ_m	a	b
$\rightarrow C_0$	C_1	C_1
C_1	C_3	C_2
C_2	C_2	C_2
$*C_3$	C_3	C_3





El proceso anterior también se puede describir mediante una tabla como:

δ	a	b
$\{q_2, q_6\}$	$\{q_2, q_6\} \subseteq C_{01}$	$\{q_2, q_6\} \subseteq C_{01}$
$\{q_0, q_1, q_4, q_5\}$	$\{q_1, q_2, q_4, q_6\} \not\subseteq C_{0j}$	
$\{q_0, q_4\}$	$\{q_1, q_4\} \not\subseteq C_{1j}$	
$\{q_0\}$	$\{q_1\} \subseteq C_{24}$	$\{q_5\} \subseteq C_{24}$
$\{q_4\}$	$\{q_4\} \subseteq C_{23}$	$\{q_4\} \subseteq C_{23}$
$\{q_1, q_5\}$	$\{q_2, q_6\} \subseteq C_{21}$	$\{q_4\} \subseteq C_{23}$

De manera formal el AFD mínimo equivalente se expresa como:

$$M_m = (Q_m, \sum, q_{0m}, \delta_m, F_m),$$

donde

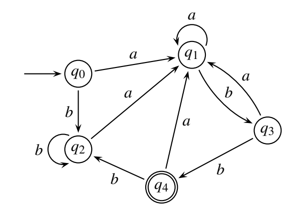
$$Q_m = Q/E, \quad \sum = \{a, b\}, \quad q_{0m} = C_0, \quad F_m = \{C_3\}$$

y δ_m como se definió anteriormente.

Ejemplo

Minimizar el autómata finito $M = (\{q_0, q_1, q_2, q_3, q_4\}, \{a, b\}, q_0, \delta, \{q_4\})$, definido por

δ	a	b
$\rightarrow q_0$	q_1	q_2
q_1	q_1	q_3
q_2	q_1	q_2
q_3	q_1	q_4
$*q_4$	q_1	q_2



Solución

Observamos que todos los estados son accesibles. Empezamos el proceso con:

$Q/E_0 = \{C_{01} = \{q_4\}, C_{02} = \{q_0, q_1, q_2, q_3\}\}$
$\delta(C_{02}, a) = \{q_1\} \subseteq C_{02}$.
$\delta(C_{02}, b) = \{q_2, q_3, q_4\} \not\subseteq C_{0j}, \ \forall j \in \{1, 2\}$.
$C_{02} = C_{021} \cup C_{022}, \ \ C_{021} = \{q_0, q_1, q_2\}, \ \ C_{022} = \{q_3\}$

$$Q/E_1 = \{C_{11} = \{q_4\}, C_{12} = \{q_3\}, C_{13} = \{q_0, q_1, q_2\}\}$$

Como $Q/E_0 \neq Q/E_1$, el proceso continúa.

$\delta(C_{13}, a) = \{q_1\} \subseteq C_{13}$

$\delta(C_{13}, b) = \{q_2, q_3\} \not\subset C_{1j}, \ \forall j \in \{1, 2, 3\}$
$C_{13} = C_{131} \cup C_{132}, \ \ C_{131} = \{q_0, q_2\}, \ \ C_{132} = \{q_1\}$

$$Q/E_2 = \{C_{21} = \{q_4\}, C_{22} = \{q_3\}, C_{23} = \{q_1\}, C_{24} = \{q_0, q_2\}\}$$

Como $Q/E_1 \neq Q/E_2$, el proceso sigue.

$\delta(C_{24}, a) = \{q_1\} \subseteq C_{23}$
$\delta(C_{24}, b) = \{q_2\} \subseteq C_{24}$

Recuerde que las clases que tienen un solo elemento no es necesario comprobarla.

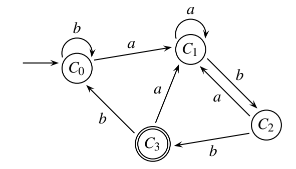
$$Q/E_3 = \{C_{31} = \{q_4\}, C_{32} = \{q_3\}, C_{33} = \{q_1\}, C_{34} = \{q_0, q_2\}\}$$

Como $Q/E_2 = Q/E_3$, se tiene que $Q/E = Q/E_2$. Luego,

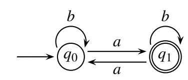
$$Q/E = \{C_0 = \{q_0, q_2\}, C_1 = \{q_1\}, C_2 = \{q_3\}, C_3 = \{q_4\}.$$

Por tanto, la tabla y el diagrama de transición del AFD mínimo equivalente son:

δ_m	a	b
$\rightarrow C_0$	C_1	C_0
C_1	C_1	C_2
C_2	C_1	C_3
$*C_3$	C_1	C_0



1. ¿Qué lenguaje reconoce el AFD dado por el diagrama de transición siguiente?:



2. Minimice el AFD $M = (Q, \sum, q_0, \delta, F)$, definido por la tabla de transición

δ	a	b
$\rightarrow q_0$	q_2	q_1
q_1	q_2	q_1
$*q_2$	q_3	q_4
$*q_3$	q_2	q_4
q_4	q_4	q_1
q_5	q_5	q_0

3. Minimice el AFD $M = (Q, \sum, q_0, \delta, F)$, definido por la tabla de transición

δ	a	b
$\rightarrow q_0$	q_4	q_1
$*q_1$	q_1	q_2
$*q_2$	q_3	q_1
$*q_3$	q_3	q_3
q_4	q_4	q_5
q_5	q_4	q_6
q_6	q_6	q_5

4. Minimice el $AFD\ M = (Q, \sum, q_0, \delta, F)$, definido por la tabla de transición

δ	a	b
$\rightarrow q_0$	q_1	q_0
$*q_1$	q_2	q_0
$*q_2$	q_1	q_0
q_3	q_0	q_0
q_4	q_2	q_4

Definición

Un autómata finito no determinista ($AFND$), M, es una 5-$tupla$, tal que

$$M = (Q, \sum, q_0, \delta, F),$$

donde

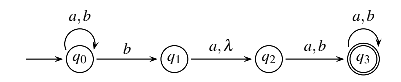
1. Q es un conjunto finito no vacío de estados.
2. $\sum$ es un alfabeto de entrada.
3. $q_0 \in Q$ es un estado inicial.
4. $F \subseteq Q$ es un conjunto de estados finales o de aceptación.
5. $\delta : Q \times (\sum \cup \lambda) \to P(Q)$ es una función asosciada a M, llamada **Función de transición.**

Notas:

1. $P(Q)$ es el conjunto potencia de Q.
2. Si $q \in Q$ y $a \in \sum$, $\delta(q, a)$ puede llevar a uno o varios estados.

Ejemplo 1

Consideremos el diagrama de transición del $AFND$ siguiente:



Observe que

1. Hay dos opciones posibles con el símbolo b desde el estado q_0.
2. Existe la posibilidad de moverse desde el estado q_1 sin leer símbolo alguno (λ).

Suponga que se tiene la entrada aba. Las posibles secuencias de estados son:

1. (q_0, q_0, q_0, q_0).
2. (q_0, q_0, q_1, q_2).
3. $(q_0, q_0, q_1, q_2, q_3)$.

Es claro que todas estas secuencias de estados son válidas. Ahora bien, ¿acepta el autómata la entrada aba?. Sí, la acepta porque alguna de las secuencias de estados conduce al estado final q_3.

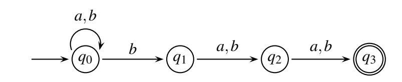
La entrada $ababba$ es también aceptada por el autómata, porque una de las posibles secuencias de estados nos lleva al estados final q_3. Sin embargo, la entrada ab es rechazada, porque no hay secuencias de estados que lleve al estado final.

El lenguaje que acepta este autómata es aquel cuyas cadenas tienen al menos un símbolo b que no es el último símbolo.

Observación: No determinismo del autómata significa que en cada momento (para cada estado y cada símbolo de entrada) pueden existir varias posibilidades de transición o incluso, ninguna.

Ejemplo 2

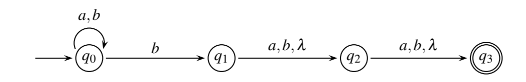
Considere el $AFND$ dado por el siguiente diagrama de transición



Este autómata acepta el lenguaje, cuyas cadenas tienen el símbolo b como antepenúltimo símbolo.

Ejemplo 3

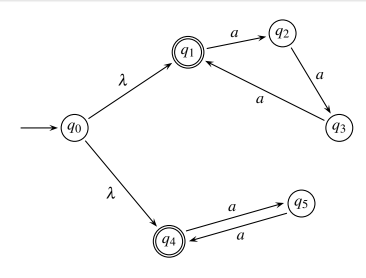
Considere el $AFND$ dado por el siguiente diagrama de transición



Este autómata acepta el lenguaje, cuyas cadenas tienen el símbolo b como último, penúltimo o antepenúltimo símbolo.

Ejemplo 4

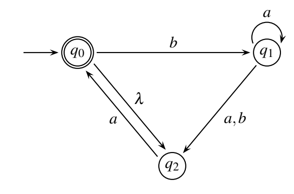
Considere el $AFND$ dado por el siguiente diagrama de transición



Este autómata acepta el lenguaje, cuyas cadenas tienen la forma de la expresión regular $(aa)^* \cup (aaa)^*$.

Ejemplo 5

Considere el $AFND$ dado por el siguiente diagrama de transición



Este autómata acepta el lenguaje, cuyas cadenas tienen la forma de la expresión regular $(a \cup ba^*ba)^*$. Estas cadenas tienen un número par de b'_s y después de cada b par tienen una a y la cadena vacía.

Ejemplo 6

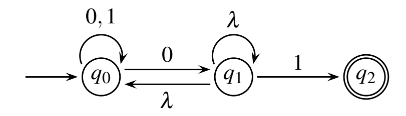
Consideremos el $AFND$ $M = (\{q_0, q_1, q_2\}, \{0, 1\}, q_0, \delta, \{q_2\})$, donde la función de transición δ se define como

$$\begin{array}{lll} \delta(q_0, 0) = \{q_0, q_1\} & \delta(q_1, 0) = \emptyset & \delta(q_2, 0) = \emptyset \\ \delta(q_0, 1) = \{q_0\} & \delta(q_1, 1) = \{q_2\} & \delta(q_2, 1) = \emptyset \\ \delta(q_0, \lambda) = \emptyset & \delta(q_1, \lambda) = \{q_0, q_1\} & \delta(q_2, \lambda) = \emptyset \end{array}$$

o mediante su tabla de transición

δ	0	1	λ
$\to q_0$	$\{q_0, q_1\}$	$\{q_0\}$	
q_1		$\{q_2\}$	$\{q_0, q_1\}$
$*q_2$			

Su diagrama de transición es



El lenguaje aceptado por el autómata M es

$$L(M) = \{\omega \in \{0,1\}^* \,|\, \omega \text{ termina en } 01\}.$$

Otro ejemplo de autómata finito no determinista ($AFND$) es $M = (Q, \sum, q_0, \delta, F)$, donde

$$Q = \{q_0, q_1, q_2, q_3\}, \;\; \sum = \{a, b, \lambda\}, \;\; F = \{q_0\}$$

y δ definida como

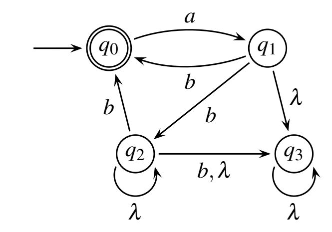
$$\begin{array}{llll} \delta(q_0, a) = \{q_1\} & \delta(q_1, a) = \emptyset & \delta(q_2, a) = \emptyset & \delta(q_3, a) = \emptyset \\ \delta(q_0, b) = \emptyset & \delta(q_1, b) = \{q_0, q_2\} & \delta(q_2, b) = \{q_0, q_3\} & \delta(q_3, b) = \emptyset \\ \delta(q_0, \lambda) = \emptyset & \delta(q_1, \lambda) = \{q_3\} & \delta(q_2, \lambda) = \{q_2, q_3\} & \delta(q_3, \lambda) = \{q_2\} \end{array}$$

Autómatas finitos no deterministas ($AFND$)

La tabla de transición es

δ	a	b	λ
$\rightarrow *q_0$	$\{q_1\}$		
q_1		$\{q_0, q_2\}$	$\{q_3\}$
q_2		$\{q_0, q_3\}$	$\{q_2, q_3\}$
q_3			$\{q_2\}$

El diagrama de transición es:



Observación:

En los autómatas finitos no deterministas, las no determinaciones cuando falten transiciones para algunas entradas se resuelven incluyendo un estado nuevo, llamado **Estado de absorción o muerto** al cual se envían todas las transiciones no definidas.

Los $AFND$ reconocen los mismos lenguajes que los AFD.
Ejemplo 7

Consideremos el autómata finito no determinista $M = \{Q, \sum, q_0, \delta, F\}$, donde

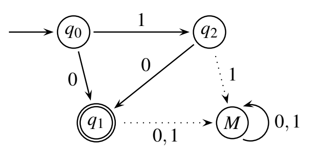
$$Q = \{q_0, q_1, q_2\}, \ \ \sum = \{0, 1\}, \ \ F = \{q_1\}.$$

La función de transición δ se define por medio de las tablas o diagrama de transición siguientes:

Tabla de transición

δ	0	1
$\rightarrow q_0$	$\{q_1\}$	$\{q_2\}$
$*q_1$		
q_2	$\{q_1\}$	

Diagrama de transición



Nueva tabla de transición

δ	0	1
$\rightarrow q_0$	$\{q_1\}$	$\{q_2\}$
$*q_1$	M	M
q_2	$\{q_1\}$	M
M	M	M

Definición

La extensión de la función de transición δ a cadenas es la función

$$\delta' : Q \times \sum^{*} \to P(Q),$$

definida como sigue:

$\forall q \in Q, \;\; x \in \sum^{*}, \;\; a \in \sum, \;\; w = xa$, se tiene que:

1. Paso base: $\delta'(q, \lambda) = \{q\}$.
2. Paso inductivo:

   Suponer que

   $\delta'(q, x) = \{q_1, q_2, \ldots, q_k\}$ y $\bigcup\limits_{i=1}^{k} \delta(q_i, a) = \{r_1, r_2, \ldots, r_m\}$.

3. Entonces $\delta'(q, w) = \{r_1, r_2, \ldots, r_m\}$.

La función δ' puede extenderse para operar sobre conjuntos de estados, de tal modo que

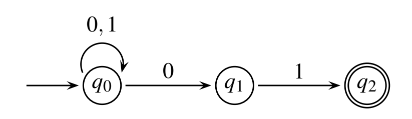
$$\forall P \subseteq Q : \delta'(P, x) = \bigcup_{p \in P} \delta'(p, x).$$

Ejemplo 8

Consideremos el $AFND\ M = (\{q_0, q_1, q_2\}, \{0, 1\}, q_0, \delta, \{q_2\})$, cuya tabla y diagrama de transición vienen dados por

δ	0	1
$\rightarrow q_0$	$\{q_0, q_1\}$	$\{q_0\}$
q_1		$\{q_2\}$
$*q_2$		

y



El lenguaje aceptado por el $AFND$ M es

$$L(M) = \{\omega \in \{0,1\}^* \,|\, \omega \text{ termina en } 01\}.$$

Ahora, suponga que queremos procesar la cadena 00101. Los pasos que debemos dar son:

1. $\delta'(q_0, \lambda) = \{q_0\}$
2. $\delta'(q_0, 0) = \delta(q_0, 0) = \{q_0, q_1\}$

3. $\delta'(q_0, 00) = \delta(q_0, 0) \cup \delta(q_1, 0) = \{q_0, q_1\} \cup \emptyset = \{q_0, q_1\}$
4. $\delta'(q_0, 001) = \delta(q_0, 1) \cup \delta(q_1, 1) = \{q_0\} \cup \{q_2\} = \{q_0, q_2\}$
5. $\delta'(q_0, 0010) = \delta(q_0, 0) \cup \delta(q_2, 0) = \{q_0, q_1\} \cup \emptyset = \{q_0, q_1\}$
6. $\delta'(q_0, 00101) = \delta(q_0, 1) \cup \delta(q_1, 1) = \{q_0\} \cup \{q_2\} = \{q_0, q_2\}$

Como $\delta'(q_0, 00101)$ tiene al menos un estado de aceptación (final), se tiene que la cadena es aceptada. Es decir, $\delta'(q_0, 00101) \cap F \neq \emptyset$.

1. Considere el $AFND$ definido por la tabla de transición

δ	0	λ
$\rightarrow q_0$	$\{q_1, q_4\}$	
q_1	$\{q_2\}$	
q_2	$\{q_3\}$	
$*q_3$		
q_4	$\{q_5\}$	
$*q_5$	$\{q_4\}$	

¿Qué palabras acepta este $AFND$?.

2. Considere el $AFND$ definido por la tabla de transición

δ	a	b	λ
$\rightarrow *q_0$	$\{q_1\}$		
q_1	$\{q_1, q_2, q_3\}$	$\{q_0, q_2\}$	$\{q_3\}$
q_2		$\{q_0, q_3\}$	$\{q_2, q_3\}$
$*q_3$			$\{q_2\}$

¿Acepta este $AFND$ la palabra a?.

Definición (λ-clausura)

La **Clausura de un estado** q respecto a λ ($C_\lambda(q)$) se define recursivamente como:

1. $q \in C_\lambda(q)$
2. Si $r \in C_\lambda(q)$ y $s \in \delta(r, \lambda)$ entonces $s \in C_\lambda(q)$

En otras palabras, es el conjunto de estados que se pueden alcanzar desde el estado q, sin consumir símbolos.

Si $P \subseteq Q$, entonces $C_\lambda(P) = \underset{p \in P}{\cup} C_\lambda(p)$.

Ejemplo 9

Consideremos el $AFND$ definido por la siguiente tabla de transición. Encuentre la clausura respecto a λ de cada uno de los estados q_0, q_1, q_2, q_3.

δ	a	b	λ
$\rightarrow *q_0$	$\{q_1\}$		
q_1	$\{q_1, q_2, q_3\}$	$\{q_0, q_2\}$	$\{q_3\}$
q_2		$\{q_0, q_3\}$	$\{q_2, q_3\}$
$*q_3$			$\{q_2\}$

Solución

$C_\lambda(q_0) = \{q_0\}$

$C_\lambda(q_1) = \{q_1\}, \;\; \delta(q_1, \lambda) = \{q_3\}, \;\; C_\lambda(q_1) = \{q_1, q_3\}$

$\delta(q_3, \lambda) = \{q_2\}, \;\; C_\lambda(q_1) = \{q_1, q_2, q_3\}, \;\; \delta(q_2, \lambda) = \{q_2, q_3\} \subseteq C_\lambda(q_1)$

Luego, $C_\lambda(q_1) = \{q_1, q_2, q_3\}$

$C_\lambda(q_2) = \{q_2\}, \;\; \delta(q_2, \lambda) = \{q_2, q_3\}, \;\; C_\lambda(q_2) = \{q_2, q_3\}$

$\delta(q_3, \lambda) = \{q_2\} \subseteq C_\lambda(q_2)$

Luego, $C_\lambda(q_2) = \{q_2, q_3\}$

$C_\lambda(q_3) = \{q_3\}, \;\; \delta(q_3, \lambda) = \{q_2\}, \;\; C_\lambda(q_3) = \{q_2, q_3\}$

$\delta(q_2, \lambda) = \{q_2, q_3\} \subseteq C_\lambda(q_3)$

Luego, $C_\lambda(q_3) = \{q_2, q_3\}$

Definición

La extensión de la función de transición δ a cadenas es la función

$$\delta' : Q \times \sum^{*} \cup \{\lambda\} \to P(Q),$$

definida como sigue:

$\forall q \in Q, \;\; x \in \sum^{*}, \;\; a \in \sum, \;\; w = xa$, se tiene que:

1. Paso base: $\delta'(q, \lambda) = C_{\lambda}(q)$.
2. Paso inductivo:

   Suponer que:

   $\delta'(q, x) = \{q_1, q_2, \ldots, q_k\}$ y $\bigcup\limits_{i=1}^{k} \delta(q_i, a) = \{r_1, r_2, \ldots, r_m\}$.

3. Entonces $\delta'(q, w) = \bigcup\limits_{i=1}^{m} C_\lambda(r_i)$

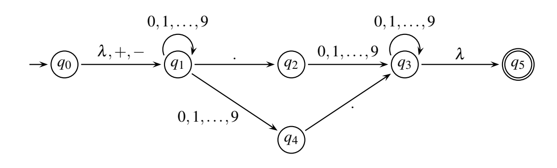
La función δ' puede extenderse para operar sobre conjuntos de estados, de tal modo que

$$\forall P \subseteq Q : \delta'(P, x) = \bigcup_{p \in P} \delta'(p, x).$$

Ejemplo

Considere el $AFND$ definido por el diagrama de transición siguiente:

Función de transición asociada a cadenas: clausura



La tabla de transición del autómata anterior es:

δ	$+, -$	$.$	$0, 1, \ldots, 9$	λ
$\to q_0$	$\{q_1\}$	$\emptyset$	$\emptyset$	$\{q_1\}$
q_1	$\emptyset$	$\{q_2\}$	$\{q_1, q_4\}$	$\emptyset$
q_2	$\emptyset$	$\emptyset$	$\{q_3\}$	$\emptyset$
q_3	$\emptyset$	$\emptyset$	$\{q_3\}$	$\{q_5\}$
q_4	$\emptyset$	$\{q_3\}$	$\emptyset$	$\emptyset$
$*q_5$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

Verificar si la cadena 7.58 es aceptada por el autómata. Es decir, si

$$\delta'(q_0, 7.58) \cap F \neq \emptyset.$$

$\delta(q_0, \lambda) = C_\lambda(q_0) = \{q_0, q_1\}$

$\delta(q_0, 7) \cup \delta(q_1, 7) = \emptyset \cup \{q_1, q_4\} = \{q_1, q_4\}$

$\delta'(q_0, 7) = C_\lambda(q_1) \cup C_\lambda(q_4) = \{q_1\} \cup \{q_4\} = \{q_1, q_4\}$

$\delta(q_1, .) \cup \delta(q_4, .) = \{q_2\} \cup \{q_3\} = \{q_2, q_3\}$

$\delta'(q_0, 7.) = C_\lambda(q_2) \cup C_\lambda(q_3) = \{q_2\} \cup \{q_3, q_5\} = \{q_2, q_3, q_5\}$

$\delta(q_2, 5) \cup \delta(q_3, 5) \cup \delta(q_5, 5) = \{q_3\} \cup \{q_3\} \cup \emptyset = \{q_3\}$

$\delta'(q_0, 7.5) = C_\lambda(q_3) = \{q_3, q_5\}$

$\delta(q_3, 8) \cup \delta(q_5, 8) = \{q_3\} \cup \emptyset = \{q_3\}$

$\delta'(q_0, 7.58) = C_\lambda(q_3) = \{q_3, q_5\}$

Como $\{q_3, q_5\} \cap F \neq \emptyset$, la cadena 7.58 es aceptada por el autómata.

Ejercicios

1. Verifique si la cadena $56 - 34$ es aceptada por el autómata.
2. Verifique si la cadena $3.2 + 4.8$ es aceptada por el autómata.

La ventaja de los $AFND$ es que son más sencillos y simples que los AFD. La ventaja de los AFD es que son más fáciles de analizar y simplificar que los $AFND$.

Definición (reconocimiento de lenguajes)

Sea $M = (Q, \sum, q_0, \delta, F)$ un $AFND$. El lenguaje reconocido por M es el conjunto de palabras que pueden hacer caminar el autómata desde el estado q_0 hasta un estado final. Es decir,

$$L(M) = \left\{ \omega \,|\, \omega \in \sum^*, \, \delta'(q_0, \omega) \cap F \neq \emptyset \right\}.$$

Ejemplo 10

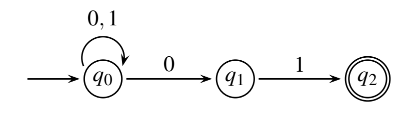
Consideremos el $AFND\ M_1 = (\{q_0, q_1, q_2\}, \{0, 1\}, q_0, \delta, \{q_2\})$, donde la función de transición δ se define como

$$\begin{array}{lll} \delta(q_0, 0) = \{q_0, q_1\} & \delta(q_1, 0) = \emptyset & \delta(q_2, 0) = \emptyset \\ \delta(q_0, 1) = \{q_0\} & \delta(q_1, 1) = \{q_2\} & \delta(q_2, 1) = \emptyset \end{array}$$

o mediante su tabla de transición

δ	0	1
$\rightarrow q_0$	$\{q_0, q_1\}$	$\{q_0\}$
q_1		$\{q_2\}$
$*q_2$		

Su diagrama de transición es



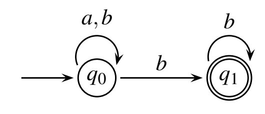
El lenguaje aceptado por el $AFND$ M es

$$L(M) = \{\omega \in \{0,1\}^* \,|\, \omega \text{ termina en } 01\},$$

como vimos anteriormente.

Ejemplo 11

Consideremos el $AFND$ $M = (\{q_0, q_1\}, \{a, b\}, q_0, \delta, \{q_1\})$, donde el diagrama de transición es:



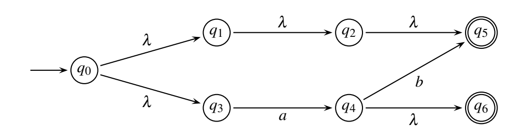
Este autómata reconoce el lenguaje, cuyas palabras terminan en b. Es decir, el lenguaje regular definido por la expresión regular $\{a \cup b\}^* b^+$.

Definición (equivalencia)

Los autómatas M_1 y M_2 son **Equivalentes** ($M_1 \equiv M_2$) si reconocen el mismo lenguaje. Es decir, si

$$L(M_1) = L(M_2).$$

1. Considere el $AFND$ definido por el diagrama de transición siguiente:



Encuentre la clausura con respecto a λ de cada uno de los estados del autómata.

2. Considere el $AFND$ del ejemplo 9 para encontrar los valores de $\delta'(q_0, b),\ \delta'(q_1, b),\ \delta'(q_0, a),\ \delta'(q_0, ba),\ \delta'(q_0, aa),\ \delta'(q_0, aab),\ \delta'(q_2, \lambda)$.
3. Considere el $AFND$ del ejemplo 10 para encontrar los valores de $\delta'(q_0, 00100),\ \delta'(q_0, 001001),\ \delta'(q_0, 0101)$.

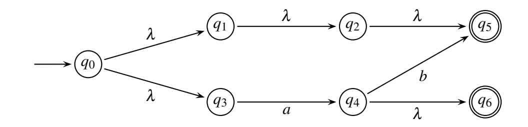
Conversión de un $AFND - \lambda$ a un $AFND$

Las transiciones vacías se eliminan con el siguiente algoritmo:

1. Calcular $C_\lambda(q_0)$. Este conjunto es el estado inicial del nuevo autómata.
2. $\forall a \in \sum$, se obtienen los estados alcanzables $q \in Q$ desde algún estado de $C_\lambda(q_0)$ y se calcula $C_\lambda(q)$. Si las $C_\lambda(q)$ producen nuevos conjuntos diferentes de $C_\lambda(q_0)$, estos serán nuevos estados a los que se accederá a partir de $C_\lambda(q_0)$ y del símbolo correspondiente.
3. Se repite el paso 2 para cada conjunto nuevo, hasta que no existan transiciones posibles para algún símbolo de $\sum$.

Ejemplo

Considere el $AFND - \lambda$ $M = (Q, \sum, q_0, \delta, F)$ dado por el diagrama de transición siguiente:



Para obtener el $AFND$, empezamos calculando $C_\lambda(q_0)$.

$C_\lambda(q_0) = \{q_0, q_1, q_2, q_3, q_5\} = E_0$

Observemos que para los símbolos a y b desde los estados q_0, q_1, q_2, q_5 de $C_\lambda(q_0)$ no hay estados alcanzables (no hay transiciones posibles). Sin embargo, desde el estado q_3 con el símbolo a se alcanza el estado q_4. Con el símbolo b, no hay transiciones posibles.

Ahora, calculamos $C_\lambda(q_4)$.

$C_\lambda(q_4) = \{q_4, q_6\} = E_1$. Este es un nuevo conjunto, por tanto, un estado nuevo.

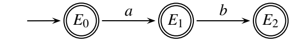
Para los símbolos a y b desde el estado q_6, no hay estados alcanzables (no hay transiciones posibles). Sin embargo, desde el estado q_4 con el símbolo b, se alcanza el estado q_5.

Ahora, calculamos $C_\lambda(q_5)$.

$C_\lambda(q_5) = \{q_5\} = E_2$. Este es un nuevo conjunto, por tanto, un nuevo estado. Desde este estado, para los símbolos a y b, no hay estados alcanzables (no hay transiciones posibles).

Luego, el $AFND$ sin transiciones vacías consta de los estados $E_0 = \{q_0, q_1, q_2, q_3, q_5\}$, $E_1 = \{q_4, q_6\}$, y $E_2 = \{q_5\}$.

Su diagrama de transición es:



Nota: Cuando la única razón del no determinismo es la presencia de transiciones λ, el $AFND$ resulta ser un AFD como en el caso anterior.

Contenido

Todo $AFND$ tiene un AFD equivalente. Es decir, todo lenguaje que se pueda describir mediante un $AFND$, se puede describir también mediante un AFD. En otras palabras, reconocen el mismo lenguaje.

Teorema

Dado un $AFND$ $M_1 = (Q, \sum, q_{10}, \delta_1, F_1)$ existe un AFD M_2, tal que $L(M_1) = L(M_2)$.

Demostración

Consideremos el AFD $M_2 = (P(Q), \sum, q_{20}, \delta_2, F_2)$, donde

1. $q_{20} = \delta_1(q_{10}, \lambda) = C_\lambda(q_{10})$
2. $F_2 = \{c \,|\, c \in P(Q) \text{ y } c \cap F_1 \neq \emptyset\}$

3. $\delta_2(c_i, a) = \bigcup_{p \in c_i} \delta_1(p, a)$

Observemos que para todo $x \in \sum^*$, $x \in L(M_1)$, si y sólo si, $x \in L(M_2)$. Es decir,

$$\begin{array}{lcll} x \in L(M_1) & \Leftrightarrow & \delta_1'(q_{10}, x) \cap F_1 \neq \emptyset & \text{(Leng. reconocido por } AFND\text{)} \\ & \Leftrightarrow & \delta_1'(q_{10}, x) \in F_2 & \text{(Por def. de } F_2\text{)} \\ & \Leftrightarrow & \delta_2'(q_{20}, x) \in F_2 & \text{(Por def. de } q_{20} \text{ y } \delta_2\text{)} \\ & \Leftrightarrow & x \in L(M_2) & \end{array}$$

Por tanto, $M_2 = M_1$.

Ejemplo

Consideremos el $AFND$ del ejemplo anterior. Construyamos un AFD equivalente.

Observemos que el conjunto de estados del AFD es $P(Q)$ (conjunto potencia de Q), que en este caso tiene 2^3 elementos. Los símbolos de entrada son los mismos. El estado de inicio es el conjunto, cuyo único elemento es q_0. El conjunto de estados finales es el conjunto de los elementos de $P(Q)$, cuya intercepción con el conjunto de estados finales del $AFND$ es no vacía.

Así que la tabla de transiciones del AFD equivalente al $AFND$ dado es :

δ_2	0	1
$\emptyset$	$\emptyset$	$\emptyset$
$\rightarrow \{q_0\}$	$\{q_0, q_1\}$	$\{q_0\}$
$\{q_1\}$	$\emptyset$	$\{q_2\}$
$*\{q_2\}$	$\emptyset$	$\emptyset$
$\{q_0, q_1\}$	$\{q_0, q_1\}$	$\{q_0, q_2\}$
$*\{q_0, q_2\}$	$\{q_0, q_1\}$	$\{q_0\}$
$*\{q_1, q_2\}$	$\emptyset$	$\{q_2\}$
$*\{q_1, q_2, q_3\}$	$\{q_0, q_1\}$	$\{q_0, q_2\}$

Esta tabla de transiciones corresponde a un AFD, aunque sus elementos sean conjuntos. Lo que ocurre es que estos conjuntos se

consideran como un estado individual y pueden ser renombrados con otros símbolos. Por ejemplo, el conjunto $\emptyset$ se le puede llamar $E_\emptyset$, el conjunto $\{q_0\}$ se puede renombrar por E_0 y así sucesivamente. De este modo la tabla de transiciones toma la forma:

δ_2	0	1
$E_\emptyset$	$E_\emptyset$	$E_\emptyset$
$\rightarrow E_0$	E_3	E_0
E_1	$E_\emptyset$	E_2
$*E_2$	$E_\emptyset$	$E_\emptyset$
E_3	E_3	E_4
$*E_4$	E_3	E_0
$*E_5$	$E_\emptyset$	E_2
$*E_6$	E_3	E_4

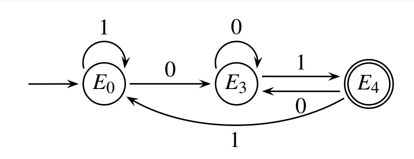
Este AFD no tiene por qué ser mínimo, incluso puede tener una gran cantidad de estados inaccesibles (no conexo). Si vemos el AFD anterior nos damos cuenta de que desde el estado inicial E_0 sólo se puede alcanzar los estados E_0, E_3 y E_4. Los demás estados se pueden eliminar, obteniéndose el AFD:

δ_2	0	1
$\rightarrow E_0$	E_3	E_0
E_3	E_3	E_4
$*E_4$	E_3	E_0

o

δ_2	0	1
$\rightarrow \{q_0\}$	$\{q_0, q_1\}$	$\{q_0\}$
$\{q_0, q_1\}$	$\{q_0, q_1\}$	$\{q_0, q_2\}$
$*\{q_0, q_2\}$	$\{q_0, q_1\}$	$\{q_0\}$

El diagrama de transición del AFD anterior es el siguiente:



Teorema

Dado un AFD $M_1 = (Q, \sum, q_0, \delta_1, F)$, existe un $AFND$ M_2, tal que $L(M_1) = L(M_2)$.

Demostración

Esta demostración es sencilla, puesto que todo AFD puede extenderse a un $AFND$. Consideremos el $AFND$ $M_2 = (Q, \sum, q_0, \delta_2, F)$, de modo que

1. $\delta_2(q, \lambda) = \emptyset, \forall q \in Q$.
2. $\delta_2(q, a) = \{\delta_1(q, a)\}, \forall q \in Q,$ y $a \in \sum$.

Es claro que $L(M_1) = L(M_2)$ y por tanto, $M_1 \equiv M_2$.

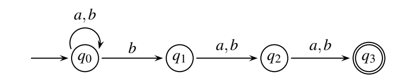
Método para hallar un AFD desde un $AFND$ sin λ-transiciones (evaluación perezosa)

1. Construir una tabla con una columna para δ_2 y una columna para cada $a \in \sum$.
2. En la primera fila y primera columna, escribir $\{q_0\}$ y en cada columna $a \in \sum$, escribir $\delta_1(\{q_0\}, a)$. Es decir, todos los estados que se pueden alcanzar desde q_0 con entrada a.
3. Copiar los resultados que están en las celdas de la fila anterior como inicio de nuevas filas.
4. Para cada fila R pendiente, rellenar la fila R, escribiendo en cada columna $a \in \sum$, $\delta_1(R, a)$. Es decir, todos los estados a los que se puede alcanzar desde algún estado de R con entrada a.

5. Copiar los resultados que están en las celdas de la fila anterior como inicio de nuevas filas.
6. Repetir los pasos 4 y 5 hasta que no queden filas por rellenar.

Ejemplo

Considere el $AFND$ definido por el siguiente diagrama de transición:



Método para hallar un AFD desde un $AFND$ sin λ-transiciones

Aplicando el método descrito anteriormente, obtenemos la siguiente tabla de transición del AFD equivalente:

δ_2	a	b
$\rightarrow \{q_0\}$	$\{q_0\}$	$\{q_0, q_1\}$
$\{q_0, q_1\}$	$\{q_0, q_2\}$	$\{q_0, q_1, q_2\}$
$\{q_0, q_2\}$	$\{q_0, q_3\}$	$\{q_0, q_1, q_3\}$
$\{q_0, q_1, q_2\}$	$\{q_0, q_2, q_3\}$	$\{q_0, q_1, q_2, q_3\}$
$*\{q_0, q_3\}$	$\{q_0\}$	$\{q_0, q_1\}$
$*\{q_0, q_1, q_3\}$	$\{q_0, q_2\}$	$\{q_0, q_1, q_2\}$
$*\{q_0, q_2, q_3\}$	$\{q_0, q_3\}$	$\{q_0, q_1, q_3\}$
$*\{q_0, q_1, q_2, q_3\}$	$\{q_0, q_2, q_3\}$	$\{q_0, q_1, q_2, q_3\}$

Esta tabla fue generada por los cálculos siguientes:

$\delta_1(q_0, a) = \{q_0\}, \quad \delta_1(q_0, b) = \{q_0, q_1\}$

$$\begin{aligned}
\delta_1(\{q_0, q_1\}, a) &= \delta_1(q_0, a) \cup \delta_1(q_1, a) = \{q_0\} \cup \{q_2\} = \{q_0, q_2\} \\
\delta_1(\{q_0, q_1\}, b) &= \delta_1(q_0, b) \cup \delta_1(q_1, b) = \{q_0, q_1\} \cup \{q_2\} = \{q_0, q_1, q_2\}
\end{aligned}$$

$$\begin{aligned}
\delta_1(\{q_0, q_2\}, a) &= \delta_1(q_0, a) \cup \delta_1(q_2, a) = \{q_0\} \cup \{q_3\} = \{q_0, q_3\} \\
\delta_1(\{q_0, q_2\}, b) &= \delta_1(q_0, b) \cup \delta_1(q_2, b) = \{q_0, q_1\} \cup \{q_3\} = \{q_0, q_1, q_3\}
\end{aligned}$$

Método para hallar un AFD desde un $AFND$ sin λ-transiciones

$$
\begin{aligned}
\delta_1(\{q_0,q_1,q_2\},a) &= \delta_1(q_0,a)\cup\delta_1(q_1,a)\cup\delta_1(q_2,a)\\
&= \{q_0\}\cup\{q_2\}\cup\{q_3\}=\{q_0,q_2,q_3\}\\
\delta_1(\{q_0,q_1,q_2\},b) &= \delta_1(q_0,b)\cup\delta_1(q_1,b)\cup\delta_1(q_2,b)\\
&= \{q_0,q_1\}\cup\{q_2\}\cup\{q_3\}=\{q_0,q_1,q_2,q_3\}
\end{aligned}
$$

$$
\begin{aligned}
\delta_1(\{q_0,q_3\},a) &= \delta_1(q_0,a)\cup\delta_1(q_3,a)=\{q_0\}\cup\emptyset=\{q_0\}\\
\delta_1(\{q_0,q_3\},b) &= \delta_1(q_0,b)\cup\delta_1(q_3,b)=\{q_0,q_1\}\cup\emptyset=\{q_0,q_1\}
\end{aligned}
$$

Método para hallar un AFD desde un $AFND$ sin λ-transiciones

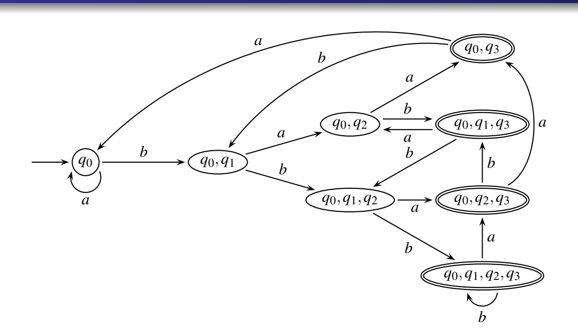
$$\begin{aligned}
\delta_1(\{q_0, q_1, q_3\}, a) &= \delta_1(q_0, a) \cup \delta_1(q_1, a) \cup \delta_1(q_3, a) \\
&= \{q_0\} \cup \{q_2\} \cup \emptyset = \{q_0, q_2\} \\
\delta_1(\{q_0, q_1, q_3\}, b) &= \delta_1(q_0, b) \cup \delta_1(q_1, b) \cup \delta_1(q_3, b) \\
&= \{q_0, q_1\} \cup \{q_2\} \cup \emptyset = \{q_0, q_1, q_2\}
\end{aligned}$$

$$\begin{aligned}
\delta_1(\{q_0, q_2, q_3\}, a) &= \delta_1(q_0, a) \cup \delta_1(q_2, a) \cup \delta_1(q_3, a) \\
&= \{q_0\} \cup \{q_3\} \cup \emptyset = \{q_0, q_3\} \\
\delta_1(\{q_0, q_2, q_3\}, b) &= \delta_1(q_0, b) \cup \delta_1(q_2, b) \cup \delta_1(q_3, b) \\
&= \{q_0, q_1\} \cup \{q_3\} \cup \emptyset = \{q_0, q_1, q_3\}
\end{aligned}$$

$$
\begin{aligned}
\delta_1(\{q_0, q_1, q_2, q_3\}, a) &= \delta_1(q_0, a) \cup \delta_1(q_1, a) \cup \delta_1(q_2, a) \cup \delta_1(q_3, a) \\
&= \{q_0\} \cup \{q_2\} \cup \{q_3\} \cup \emptyset = \{q_0, q_2, q_3\} \\
\delta_1(\{q_0, q_1, q_2, q_3\}, b) &= \delta_1(q_0, b) \cup \delta_1(q_1, b) \cup \delta_1(q_2, b) \cup \delta_1(q_3, b) \\
&= \{q_0, q_1\} \cup \{q_2\} \cup \{q_3\} \cup \emptyset = \{q_0, q_1, q_2, q_3\}
\end{aligned}
$$

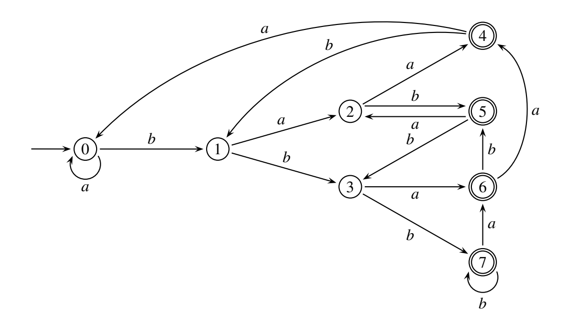
El diagrama de transición es

Método para hallar un AFD desde un $AFND$ sin λ-transiciones



Método para hallar un AFD desde un $AFND$ sin λ-transiciones

A veces es conveniente cambiar el nombre de los estados para obtener un diagrama más claro, como el siguiente:



Método para hallar un AFD desde un $AFND$ con λ-transiciones (evaluación perezosa)

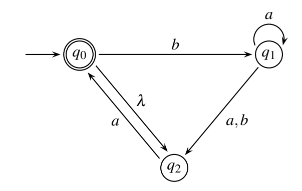
1. Construir una tabla con una columna para δ_2 y una columna para cada $a \in \sum$.
2. En la primera fila y primera columna, escribir $C_\lambda(q_0)$. Es decir, todos los estados a los que se puede llegar desde q_0 con λ^*; y en cada columna $a \in \sum$, escribir $\bigcup_{r \in C_\lambda(q_0)} C_\lambda(\delta_1(r, a))$. Es decir, todos los estados que se pueden alcanzar desde $C_\lambda(q_0)$ con entrada $a\lambda^*$.
3. Copiar los resultados que están en las celdas de la fila anterior como inicio de nuevas filas.

Método para hallar un AFD desde un $AFND$ con λ-transiciones (evaluación perezosa)

4. Para cada fila R pendiente, rellenar la fila R, escribiendo en cada columna a, $\bigcup_{r \in R} C_\lambda(\delta_1(r, a))$. Es decir, todos los estados a los que se puede alcanzar desde algún estado de R con entrada $a\lambda^*$.
5. Copiar los resultados que están en las celdas de la fila anterior como inicio de nuevas filas.
6. Repetir los pasos 4 y 5 hasta que no queden filas por rellenar.

Ejemplo

Considere el $AFND$ definido por el siguiente diagrama de transición:



Aplicando el método descrito anteriormente, se tiene que:

$C_\lambda(q_0) = \{q_0\}$, $\delta_1(q_0, \lambda) = \{q_2\}$. Luego, $C_\lambda(q_0) = \{q_0, q_2\}$.

$$\begin{aligned}\bigcup_{r\in\{q_0,q_2\}} C_\lambda(\delta_1(r,a)) &= C_\lambda(\delta_1(q_0,a)) \cup C_\lambda(\delta_1(q_2,a)) = \emptyset \cup C_\lambda(\{q_0\}) \\ &= \emptyset \cup \{q_0, q_2\} = \{q_0, q_2\}.\end{aligned}$$

$$\begin{aligned}\bigcup_{r\in\{q_0,q_2\}} C_\lambda(\delta_1(r,b)) &= C_\lambda(\delta_1(q_0,b)) \cup C_\lambda(\delta_1(q_2,b)) \\ &= C_\lambda(\{q_1\}) \cup \emptyset = \{q_1\}.\end{aligned}$$

Método para hallar un AFD desde un $AFND$ con λ-transiciones

$$\begin{aligned}
\bigcup_{r\in\{q_1\}} C_\lambda(\delta_1(r,a)) &= C_\lambda(\delta_1(q_1,a)) = C_\lambda(\{q_1,q_2\}) \\
&= C_\lambda(\{q_1\}) \cup C_\lambda(\{q_2\}) = \{q_1\} \cup \{q_2\} = \{q_1,q_2\}.
\end{aligned}$$

$$\bigcup_{r\in\{q_1\}} C_\lambda(\delta_1(r,b)) = C_\lambda(\delta_1(q_1,b)) = C_\lambda(\{q_2\}) = \{q_2\}.$$

$$\begin{aligned}
\bigcup_{r\in\{q_1,q_2\}} C_\lambda(\delta_1(r,a)) &= C_\lambda(\delta_1(q_1,a)) \cup C_\lambda(\delta_1(q_2,a) \\
&= C_\lambda(\{q_1,q_2\}) \cup C_\lambda(\{q_0\}) \\
&= C_\lambda(\{q_1\}) \cup C_\lambda(\{q_2\}) \cup C_\lambda(\{q_0\}) \\
&= \{q_1\} \cup \{q_2\} \cup \{q_0,q_2\} = \{q_0,q_1,q_2\}.
\end{aligned}$$

Método para hallar un AFD desde un $AFND$ con λ-transiciones

$$\begin{aligned}\bigcup_{r\in\{q_1,q_2\}} C_\lambda(\delta_1(r,b)) &= C_\lambda(\delta_1(q_1,b)) \cup C_\lambda(\delta_1(q_2,b)\\ &= C_\lambda(\{q_2\}) \cup C_\lambda(\emptyset) = \{q_2\} \cup \emptyset = \{q_2\}.\end{aligned}$$

$$\bigcup_{r\in\{q_2\}} C_\lambda(\delta_1(r,a)) = C_\lambda(\delta_1(q_2,a)) = C_\lambda(\{q_0\}) = \{q_0,q_2\}.$$

$$\bigcup_{r\in\{q_2\}} C_\lambda(\delta_1(r,b)) = C_\lambda(\delta_1(q_2,b)) = C_\lambda(\emptyset) = \emptyset.$$

Método para hallar un AFD desde un $AFND$ con λ-transiciones

$$
\begin{aligned}
\bigcup_{r\in\{q_0,q_1,q_2\}} C_\lambda(\delta_1(r,a)) &= C_\lambda(\delta_1(q_0,a)) \cup C_\lambda(\delta_1(q_1,a) \cup C_\lambda(\delta_1(q_2,a) \\
&= C_\lambda(\emptyset) \cup C_\lambda(\{q_1,q_2\}) \cup C_\lambda(\{q_0\}) \\
&= \emptyset \cup \{q_1,q_2\} \cup \{q_0,q_2\} = \{q_0,q_1,q_2\}.
\end{aligned}
$$

$$
\begin{aligned}
\bigcup_{r\in\{q_0,q_1,q_2\}} C_\lambda(\delta_1(r,b)) &= C_\lambda(\delta_1(q_0,b)) \cup C_\lambda(\delta_1(q_1,b) \cup C_\lambda(\delta_1(q_2,b) \\
&= C_\lambda(\{q_1\}) \cup C_\lambda(\{q_2\}) \cup C_\lambda(\emptyset) \\
&= \{q_1\} \cup \{q_2\} \cup \emptyset = \{q_1,q_2\}.
\end{aligned}
$$

Luego, la tabla de transición del AFD equivalente es :

Método para hallar un AFD desde un $AFND$ con λ-transiciones

δ_2	a	b
$\rightarrow \{q_0, q_2\}$	$\{q_0, q_2\}$	$\{q_1\}$
$\{q_1\}$	$\{q_1, q_2\}$	$\{q_2\}$
$\{q_1, q_2\}$	$\{q_0, q_1, q_2\}$	$\{q_2\}$
$\{q_2\}$	$\{q_0, q_2\}$	$\emptyset$
$*\{q_0, q_1, q_2\}$	$\{q_0, q_1, q_2\}$	$\{q_1, q_2\}$
$\emptyset$	$\emptyset$	$\emptyset$

Encuentre el AFD equivalente en cada uno de los siguientes ejercicios:

1. Considere el $AFND$ definido por la tabla de transición

δ	0	λ
$\rightarrow q_0$	$\{q_1, q_4\}$	$\emptyset$
q_1	$\{q_2\}$	$\emptyset$
q_2	$\{q_3\}$	$\emptyset$
$*q_3$	$\emptyset$	$\emptyset$
q_4	$\{q_5\}$	$\emptyset$
$*q_5$	$\{q_4\}$	$\emptyset$

2. Considere el $AFND$ definido por la tabla de transición

δ	a	b	λ
$\rightarrow *q_0$	$\{q_1\}$	$\emptyset$	$\emptyset$
q_1	$\{q_1, q_2, q_3\}$	$\{q_0, q_2\}$	$\{q_3\}$
q_2	$\emptyset$	$\{q_0, q_3\}$	$\{q_2, q_3\}$
$*q_3$	$\emptyset$	$\emptyset$	$\{q_2\}$

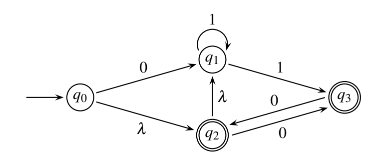
3. Considere el $AFND$ definido por la tabla de transición

δ	0	1	λ
$\rightarrow *q_0$	$\{q_1\}$	$\{q_1\}$	$\emptyset$
$*q_1$	$\{q_0, q_2\}$	$\{q_1\}$	$\{q_2\}$
q_2	$\emptyset$	$\{q_1\}$	$\emptyset$

4. Considere el $AFND$ definido por la tabla de transición

δ	0	1	λ
$\rightarrow q_0$	$\emptyset$	$\emptyset$	$\{q_1, q_3\}$
$*q_1$	$\{q_2\}$	$\{q_1\}$	$\emptyset$
q_2	$\{q_1\}$	$\{q_2\}$	$\emptyset$
$*q_3$	$\{q_3\}$	$\{q_4\}$	$\emptyset$
q_4	$\{q_4\}$	$\{q_3\}$	$\emptyset$

5. Considere el $AFND$ definido por el diagrama de transición siguiente:



6. Considere el $AFND$ definido por la tabla de transición

δ	a	b	c
$\rightarrow q_0$	$\{q_1\}$	$\emptyset$	$\emptyset$
q_1	$\emptyset$	$\{q_1\}$	$\{q_2\}$
$*q_2$	$\emptyset$	$\emptyset$	$\emptyset$

7. Considere el $AFND$ definido por la tabla de transición

δ	a	b
$\rightarrow q_0$	$\{q_1\}$	$\emptyset$
$*q_1$	$\{q_1\}$	$\{q_1\}$

8. Considere el $AFND$ definido por la tabla de transición

δ	a	b
$\rightarrow q_0$	$\{q_0, q_1\}$	$\{q_0\}$
q_1	$\{q_2\}$	$\emptyset$
$*q_2$	$\{q_2\}$	$\{q_2\}$

9. Considere el $AFND$ definido por la tabla de transición

δ	0	1
$\rightarrow q_0$	$\{q_0, q_1\}$	$\{q_0\}$
q_1	$\emptyset$	$\{q_2\}$
q_2	$\{q_3\}$	$\emptyset$
q_3	$\{q_4\}$	$\emptyset$
q_4	$\emptyset$	$\{q_5\}$
q_5	$\{q_6\}$	$\emptyset$
$*q_6$	$\{q_6\}$	$\{q_6\}$